PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-256345
(43)Date of publication of application : 17.10.1990

(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
H04N 1/44

(21)Application number : 01-077774
(22)Date of filing : 29.03.1989

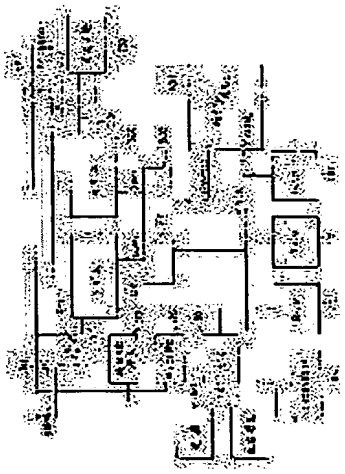
(71)Applicant : AISIN SEIKI CO LTD
(72)Inventor : KATO EIJI
NARUSE YOSHIHIRO

(54) PRIVACY COMMUNICATION CONTROLLER

(57)Abstract:

PURPOSE: To attain communication for plural number of times for transmission and reception of a key by disconnecting its own station side communication means from a communication line and transmitting and receiving the information relating to the key between privacy communication controllers connected to the communication line in that state.

CONSTITUTION: A memory card 130 is used as keys in a sense in privacy communication and freely attachable and detachable to/from a privacy equipment with a prescribed connector. The inside of the memory card 130 is provided with a battery for backing up the storage content and a read/write memory storing an ID code of the card. That is, only when the memory card having the same ID code is loaded to each privacy equipment arranged near a facsimile equipment at the sender side and the receiver side, normal privacy communication is attained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−256345

⑤Int.Cl.⁵		識別記号	庁内整理番号	⑬公開　平成2年(1990)10月17日
H 04 L	9/00			
	9/10			
	9/12			
H 04 N	1/44		6940−5C	
			6945−5K　H 04 L　9/00　Z	

審査請求　未請求　請求項の数 2　(全27頁)

⑭発明の名称　秘匿通信制御装置

⑳特　願　平1−77774
㉒出　願　平1(1989)3月29日

⑫発明者　加藤　英治　愛知県刈谷市朝日町2丁目1番地　アイシン精機株式会社内
⑫発明者　成瀬　好廣　愛知県刈谷市朝日町2丁目1番地　アイシン精機株式会社内
⑪出願人　アイシン精機株式会社　愛知県刈谷市朝日町2丁目1番地
⑭代理人　弁理士　杉信　興

明　細　書

1．発明の名称

秘匿通信制御装置

2．特許請求の範囲

(1)相手側通信手段と接続される第1組の信号線；

前記第1組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第1の変復調手段；

自局側通信手段と接続された第2組の信号線；

第3組の信号線；

前記第3組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第2の変復調手段；

前記第1の変復調手段が復調した信号を復号化して前記第2の変復調手段の変調入力端子に印加し、前記第2の変復調手段が復調した信号を暗号化して前記第1の変復調手段の変調入力端子に印加する、秘匿情報処理手段；

前記第2組の信号線を、前記第1組の信号線と前記第3組の信号線との一方に選択的に接続する切換スイッチ手段；及び

自局側通信手段が発呼側か被呼側かを自動的に識別し、発呼側の時には、第1組の信号線上で被呼局識別の信号が検出された時に、被呼側の時には、自局側通信手段が被呼局識別の信号を送出する時に、前記切換スイッチ手段を制御して自局側通信手段を第1組の信号線から遮断し、暗号化通信の鍵を決定する暗号を含む情報の受渡しを、第1の変復調手段及び第1組の信号線を介して行ない、その後で、決定された鍵に基づいて、第1組の信号線に印加される暗号化された受信情報を前記秘匿情報処理手段に通し復号化して第2組の信号線に出力し、第2組の信号線からの送信情報を前記秘匿情報処理手段に通し暗号化して第1組の信号線に出力する、電子制御手段；

を備える秘匿通信制御装置．

(2)電子制御手段は、鍵を決定する暗号の受渡しにおいて：

自局側通信手段が発呼側の時には；乱数を生成し、生成した乱数をマスタ鍵で暗号化した情報を第1組の信号線に送出し、その後で第1組の信号線に現われる情報を受信して、受信した情報を前記乱数に基づいて解読し、解読した情報と前記乱数とが一致すると、前記乱数を以後の通信で暗号通信の鍵として利用し：

自局側通信手段が被呼側の時には；第1組の信号線に現われる情報を受信して、受信した情報をマスタ鍵で解読し、解読した情報をそれ自身に基づいて暗号化し、暗号化した情報を第1組の信号線に送出する、前記請求項1記載の秘匿通信制御装置。

3．発明の詳細な説明

〔発明の目的〕

〔産業上の利用分野〕

本発明は、例えば公衆通信回線を利用して画像情報を伝送するファクシミリ装置などの通信装置において、秘匿通信を行なうために利用される秘匿通信制御装置に関する。

〔従来の技術〕

通信情報の暗号化／復号化の手段としては、従来より様々なものが提案されており、また、ファクシミリ装置においては、例えば秘匿機能を備えるものとして、特開昭59－221167号の技術が知られている。

特開昭59－221167号の装置は、秘匿機能をファクシミリ装置に内蔵するか、又は所定のインターフェースを介して、秘匿装置をファクシミリ装置に外付けする構造になっている。また、秘匿機能の有無を自動識別するために、CCITT勧告の通信制御手順に、オプション機能として規定される信号NSF（非標準機能を示す）を利用し、その信号に、秘匿機能に関する情報を付加している。

〔発明が解決しようとする課題〕

上述の装置においては、標準化されていない信号NSFによって秘匿機能の識別を行なうので、その信号に関して同一の処理を行なうごく一部の装置、即ち自局と同一の機種しか相手側装置として利用できないという不都合がある。

また、秘匿手段を、ファクシミリ装置自体に内蔵もしくは付加する構造であるため、秘匿手段を備えるには、従来の装置をそのまま利用することはできず、ファクシミリ装置の改造や設計変更が必要不可決である。

更に、非標準機能を示す信号（NSF）を利用する場合、この信号の通信装置間でのやりとりは、1往復のみしか許されていないという制約がある。秘匿通信における暗号化／復号化に利用される鍵は、通信の度に変更するのが安全性の面で望ましく、その場合、送信側と受信側の鍵を一致させるために、鍵を設定する信号を、情報通信に先立って通信装置間で受渡しする必要がある。ところが、信号NSFを利用してその受渡しを行なう場合には、受渡しを一回しかできないので、実際に暗号化／復号化に使用する生の鍵コードを、NSF信号として直接、通信回線上に流さざるを得ない。そのため、第三者が通信回線上を盗聴すれば、鍵コードを取出すことが可能であり、それに基づいて、後で送られる暗号化メッセージを解読することができるので、第三者に情報が漏れる恐れがある。

使用する鍵コード自体を暗号化して通信回線上に流せば、それの漏洩の危険が小さくなる。しかし、通信回線上に生じたノイズなどの影響で、伝送中に情報に変形が生じる可能性もある。鍵コード自体を暗号化して受渡しする場合には、1往復の情報通信だけでは、確実に鍵コードの伝達が行なわれたか否かを確認することができず、正当な通信相手同志の間であっても受信側で正規の情報を解読できない場合が生じる。また、情報の変形によって鍵コードの受渡しに失敗した場合であっても、再送動作はできないので、一旦、回線を遮断して再び接続しない限り、正常な通信はできない。

本発明は、秘匿通信における鍵コードを通信の度に更新する装置において、鍵の受渡しのための

複数回の通信を可能にすることを共通の課題とする。

〔発明の構成〕

〔課題を解決するための手段〕

上記課題を解決するため、本発明においては、相手側通信手段と接続される第１組の信号線；前記第１組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第１の変復調手段；自局側通信手段と接続された第２組の信号線；第３組の信号線；前記第３組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第２の変復調手段；前記第１の変復調手段が復調した信号を復号化して前記第２の変復調手段の変調入力端子に印加し、前記第２の変復調手段が復調した信号を暗号化して前記第１の変復調手段の変調入力端子に印加する、秘匿情報処理手段；前記第２組の信号線を、前記第１組の信号線と前記第３組の信号線との一方に選択的に接続する切換スイッチ手段；及び自局側通信手段が発呼側か被呼側かを自動的に識別し、発呼側の時には、第１組の信号線上で被呼局識別の信号が検出された時に、被呼側の時には、自局側通信手段が被呼局識別の信号を送出する時に、前記切換スイッチ手段を制御して自局側通信手段を第１組の信号線から遮断し、暗号化通信の鍵を決定する暗号を含む情報の受渡しを、第１の変復調手段及び第１組の信号線を介して行ない、その後で、決定された鍵に基づいて、第１組の信号線に印加される暗号化された受信情報を前記秘匿情報処理手段に通し復号化して第２組の信号線に出力し、第２組の信号線からの送信情報を前記秘匿情報処理手段に通し暗号化して第１組の信号線に出力する、電子制御手段；を設ける。

〔作用〕

本発明によれば、ファクシミリの通信プロトコルにおいて、ＣＣＩＴＴによって規定されたフェーズＡからフェーズＢに移行する前に、切換スイッチ手段によって、通信回線（第１組の信号線）から自局側通信手段が切離され、その状態で通信回線に接続された秘匿通信制御装置同志の間で、鍵に関する情報のやりとりが行なわれる。従ってこの場合には、鍵に関する情報の受渡しを、実質上何回でも行なうことが可能である。このため、伝送路上における情報の変形などによって、鍵の情報の受渡しが失敗した場合、その受渡しのやり直しを、回線を切断することなく実行することができる。この情報の受渡しの際には、自局側及び相手側の通信手段（ファクシミリ）は、フェーズＢに移行する前の待機状態であり、格別な不都合は生じない。

鍵の受渡しが完了した後は、その鍵に基づいて秘匿通信制御装置が、メッセージ情報の暗号化又は解読を行ないながらそれの中継を行なうことにより、秘匿通信を行なうことができる。

また、本発明の好ましい態様においては、使用される鍵コードが通信回線を盗聴する第三者に漏れるのを防止するために、鍵を決定する暗号の受渡しにおいて電子制御手段は、次のように処理する。

自局側通信手段が発呼側の場合：

乱数を生成し、生成した乱数をマスタ鍵で暗号化した情報を第１組の信号線に送出し、その後で第１組の信号線に現われる情報を受信して、受信した情報を前記乱数に基づいて解読し、解読した情報と前記乱数とが一致すると、前記乱数を以後の通信で暗号通信の鍵として利用する。

自局側通信手段が被呼側の場合：

第１組の信号線に現われる情報を受信して、受信した情報をマスタ鍵で解読し、解読した情報をそれ自身に基づいて暗号化し、暗号化した情報を第１組の信号線に送出する。

この態様によれば、使用する鍵は暗号化された形で通信回線上に現われるので、それが第三者に盗聴されたとしても、鍵の漏洩によってメッセージが解読される恐れはない。

本発明の他の目的及び特徴は、以下の、図面を参照した実施例説明により明らかになろう。

〔実施例〕

第１図に、実施例の秘匿装置を使用してファクシミリ通信を行なう場合の、通信系全体の構成を示す。

第１図を参照すると、互いに通信を行なうファクシミリ装置（ＦＡＸ）は、交換機と接続される公衆電話回線に接続されており、該電話回線に接続された各々のファクシミリと交換機との間に、それぞれ、秘匿装置が介挿されている。ここに示した各々のファクシミリは、一般に市販されている、ＣＣＩＴＴに規定されるＧ３のモードを備える装置であり、改造などは一切行なっていない。つまり、実施例の秘匿装置を電話回線上に介挿するだけで、既存のファクシミリ装置を用いて秘匿通信を行なうことができる。

第２図に、送信側と受信側にそれぞれ設けられる秘匿装置の構成の概要を示す。第２図を参照すると、送信側と受信側の秘匿装置は同一の構成になっている。即ち、各々の秘匿装置は、２つのモデム（変復調装置），制御装置（ＣＰＵ），並びに信号のバイパス，暗号化及び復号化の機能を有するユニットを備えている。

秘匿通信を行なう場合、送信側においては、ファクシミリが回線上に送出した画像情報をモデムを介して入力し、それを暗号化した情報を別のモデムを介して回線上に送り出す。受信側においては、回線上に現われる暗号化情報をモデムを介して入力し、それを復号化して送信された画像情報を再生し、再生した情報を別のモデムを介してファクシミリに接続された側の回線上に送り出す。従って、各々のファクシミリは普通の動作を行なうだけであるが、２つの秘匿装置の間の回線上では、信号は暗号化されており、秘匿通信が行なわれることになる。

次に、第３図に示される秘匿装置の構成について説明する。交換機と接続される公衆電話回線ＬＮ１，ＬＮ２と、自局ファクシミリと接続される回線ＬＦ１，ＬＦ２との間には、リレーＲＹ２が介挿されている。ファクシミリ側の回線ＬＦ１，ＬＦ２は、リレーＲＹ２の共通接点に接続され、ＲＹ２の一方の接点に電話回線ＬＮ１，ＬＮ２が接続されている。また、リレーＲＹ２の他方の接点には、秘匿装置内部の線路ＬｉＢが接続されている。この例では、リレーＲＹ２がオフの時に回線ＬＮ１，ＬＮ２と回線ＬＦ１，ＬＦ２とが接続され、ＲＹ２がオンの時に回線ＬＦ１，ＬＦ２と線路ＬｉＢとが接続される。

更に、電話回線ＬＮ１，ＬＮ２はリレーＲＹ１のノーマリオープン接点を介して、秘匿装置内部の線路ＬｉＡと接続されている。また、電話回線ＬＮ１，ＬＮ２には、極性反転検出回路２１０及び呼び出し検出回路２２０が接続されており、秘匿装置内部の線路ＬｉＢには電流供給回路２３０が接続されている。

秘匿装置のその他の構成要素としては、マイクロコンピュータ（ＣＰＵ）１００，ＲＯＭ１１０，ＲＡＭ１２０，メモリカード１３０，電源１４０，乱数発生回路１５０，入出力インターフェース（Ｉ／Ｏ）１８０，モデム３００，４００，バッファ回路５００，暗号化／復号化処理回路６００が備わっている。

２つのモデム３００，４００は、各々、CCITTのＶ２７ter 即ちＧ３規格に準拠した通信機能を備えている。

マイクロコンピュータ１００のデータバスは、バッファ５００を介してモデム３００のデータバスＤＢＭ１とモデム４００のデータバスＤＢＭ２に接続されている。従って、マイクロコンピュータ１００は、モデム３００を介して自局側のファクシミリと交信したり、モデム４００を介して相手側のファクシミリと交信することができる。また、内部のデータバス（２）によって、バッファ５００と暗号化／復号化処理回路６００とが接続されている。バッファ回路５００を制御することによって、データバス（２）は、モデム３００のデータバスＤＢＭ１、又はモデム４００のデータバスＤＢＭ２と接続できる。

従って、例えば自局側のファクシミリが送信を行なう場合、暗号化すべき画像情報は線路ＬｉＢからモデム３００に入力されて復調され、データバスＤＢＭ１からバッファ５００を通して、マイ

クロコンピュータ１００のデータバスに現われ、暗号化／復号化処理回路６００のＸグループの端子に印加される。回路６００は、Ｘグループの端子に印加されたデータを暗号化し、Ｙグループの端子を介してデータバス（２）に出力する。この暗号化されたデータは、バッファ５００を通ってデータバスＤＢＭ２に出力される。そして、モデム４００によって変調され、線路ＬｉＡから電話回線ＬＮ１，ＬＮ２に送り出される。

逆に、自局側のファクシミリが受信を行なう場合、復号化すべき暗号化された画像情報は、線路ＬｉＡからモデム４００に入力されて復調され、データバスＤＢＭ２からバッファ５００を通って、データバス（２）に現われ、暗号化／復号化処理回路６００のＹグループの端子に印加される。回路６００は、その情報を復号化、即ち解読し、解読した情報をＸグループの端子に出力する。この情報は、マイクロコンピュータ１００のデータバスを通り、バッファ５００を通って、データバスＤＢＭ１を通りモデム300に印加される。モデム３００は、その情報を変調し、線路ＬｉＢを介して、自局側のファクシミリの回線ＬＦ１，ＬＦ２に送り出す。

メモリカード１３０は、秘匿通信におけるある種の鍵として利用されるものであり、所定のコネクタにより、秘匿装置に対して着脱自在になっている。このメモリカード１３０は、内部に記憶内容保持用のバッテリと、そのカードのＩＤコードを記憶した読み書きメモリを備えている。つまり、送信側と受信側のファクシミリの近傍に配置される各々の秘匿装置に、同一のＩＤコードを有するメモリカードが装着されている場合にのみ、正常な秘匿通信が可能になる。

続いて、各回路の構成を更に詳細に説明する。第３図の各回路の詳細を、第５ａ図，第５ｂ図，第５ｃ図，第５ｄ図，第６ａ図，第６ｂ図，第７ａ図，第７ｂ図，第８図及び第９図に示す。

まず、第５ａ図を参照して説明する。この回路には、マイクロコンピュータ１００とその周辺回路要素が備わっている。ここで用いているマイクロコンピュータ１００は、ＨＤ６３Ｂ０３Ｒである。ラッチＬＴ１は、マイクロコンピュータ１００のデータバスの信号として重畳された下位８ビットのアドレス情報（Ａ７－Ａ０）を抽出するアドレスラッチとして機能する。アドレスバスには、マイクロコンピュータ１００が直接出力する上位の８ビット（ＡＤ１５－ＡＤ８）アドレスラッチＬＴ１の出力する下位８ビット（ＡＤ７－ＡＤ０）との１６ビットの信号が現われる。

マイクロコンピュータ１００に接続された各種周辺回路の各々の選択する各種チップセレクト信号は、デコーダＤＥ２と各種論理ゲート（Ｇ５，Ｇ６，Ｇ７，Ｇ８，Ｇ９）で構成されるアドレスデコーダによって生成される。つまり、周辺回路の各々に予め割り当てられたアドレスがアドレスバスに現われると、それに対応するチップセレクト信号がデコードされ、その信号がアクティブになる。

第５ｂ図には、ＲＯＭ１１０，ＲＡＭ１２０及びメモリカード１３０が示されている。これらの回路は、アドレスバス，データバス及びコントロールバスを介して、マイクロコンピュータ１００と接続されている。ＤＥ１はデコーダである。なお、メモリカード１３０は、図示しないコネクタにより、回路と着脱自在に接続されている。

第５ｃ図には、入出力インターフェース１８０が示されている。この回路には、マイクロコンピュータ１００のアドレスバス，データバス及びコントロールバスと接続された集積回路１３１と、そのポートに接続されたスイッチＳＷ１－ＳＷ６，発光ダイオードＬＥＤ１－ＬＥＤ７，ブザーＢＺ，バッファ及びドライバが備わっている。

第５ｄ図には、電源回路１４０と、乱数発生回路１５０が示されている。電源回路１４０は、商用交流電源（ＡＣ１００Ｖ）の電力を直流の各種電圧に変換する機能を備えており、これ自体には格別新しい構成は備わっていない。

一方、乱数発生回路１５０は、アナログ電圧比較回路を構成している。２つの比較入力端子の一方の電圧は安定化されており、他方の入力端子に

は、電源回路１４０の出力する脈流電圧が印加される。この脈流電圧は、交流（５０Ｈｚ）波形を全波整流したものを平滑化したものであり、その電圧は、常時微妙に変化しており、しかも電源ラインに混入した様々なノイズを含んでいる。アナログ電圧比較回路のしきい値レベルは、脈流信号のレベルが変化する範囲の中間的なレベルに設定してある。

このため、該比較回路の出力端子には、周期性の小さいパルス信号ＲＭＤが現われる。この信号ＲＭＤを順次サンプリングすることにより、サンプリングの周期にもよるが、ほぼランダムな乱数データが得られる。このようにして生成される乱数データは、この実施例では、秘匿通信を行なう際の鍵コードとして利用される。

次に、第６ａ図を参照する。この回路には、極性反転検出回路２１０，呼び出し検出回路２２０及びリレーＲＹ１，ＲＹ２が示されている。リレーＲＹ１及びＲＹ２は、それぞれ、マイクロコンピュータ１００の出力する信号ＮＣＵ－ＲＬ１およびＮＣＵ－ＲＬ２によってオン／オフ制御される。

極性反転検出回路２１０は、電話回線ＬＮ１，ＬＮ２を流れる電流の有無と電流の方向の識別を行なう。線路ＬＮ１の電流を検出するために、それぞれ、発光ダイオードとフォトトランジスタとで構成されるフォトカップラＰＣ１及びＰＣ２が備わっている。各フォトカップラの発光ダイオードは互いに逆極性で線路ＬＮ１上に介在されているので、一方の向きで電流が流れるとＰＣ１がオンしてＰＣ２がオフし、他方の向きで電流が流れるとＰＣ１がオフしてＰＣ２がオンする。電流が流れない時は２つのフォトカップラＰＣ１，ＰＣ２は共にオフになる。

電話回線においては、受話機のフックがオンの時は回線に電流が流れず、フックがオフになると電流が流れる。従って、この実施例では、いずれかの方向に電流が流れていると、フックオフ信号がアクティブになるように構成してある。２つの信号ＰＯＬ１及ＰＯＬ２は、電流の向きに応じてオン／オフする。電話回線ＬＮ１，ＬＮ２上の電圧の極性は、交換機によって反転されるので、その時の回線の極性を調べるために、この機能を設けてある。この機能は、回線ＬＮ１，ＬＮ２から自局側ファクシミリを切離し、秘匿装置に接続した時に、ファクシミリ側の回線ＬＦ１，ＬＦ２に供給する電圧の極性を、電話回線ＬＮ１，ＬＮ２と一致させるために利用される。

呼び出し検出回路２２０は、電話回線ＬＮ１，ＬＮ２上に現われる呼び出し信号を検出する機能を有する。呼び出し信号は交流信号なので、この回路においては、コンデンサによって直流成分を遮断した信号を全波整流回路に通して整流し、その整流出力に所定レベル以上の信号が現われる時に着呼信号がオンするように構成してある。

第６ｂ図には、電流供給回路２３０が示されている。この回路は、自局側のファクシミリを電話回線ＬＮ１，ＬＮ２から切離して、秘匿装置側の線路ＬｉＢに接続した時に、自局側のファクシミリ装置の回線ＬＦ１，ＬＦ２に電圧を供給する機能を有する。電圧の極性をその時の電話回線ＬＮ１，ＬＮ２における極性と一致させるために、前述の極性反転検出回路２１０が出力する極性信号ＰＯＬ１及びＰＯＬ２を利用している。

従って、仮に既存のファクシミリ装置が、それの接続された回線の電圧及び電流を監視して、その状態に応じた制御を行なっている場合でも、そのファクシミリの回線の接続を、電話回線からこの秘匿装置に切換えることによって何ら不具合が生じる恐れはない。なお、電話回線ＬＮ１，ＬＮ２においては、通常は４８Ｖの電圧が現われるが、電流供給回路２３０は２８Ｖの電圧を供給するようになっている。

第７ａ図には、モデム３００が示されている。このモデムの回路の大部分は、シングルチップの集積回路（Ｒ４８ＰＣＪ）３１０で構成されている。この集積回路３１０は、ＣＣＩＴＴのＶ２７ter に準拠した機能を備えている。基本的には、集積回路３１０の機能として、そのデータ端子（Ｄ７－Ｄ０）に印加されるデジタル信号をシリ

アル信号に変換し変調を行なってシリアル送信出力端子ＴＸＯＵＴに出力する機能と、シリアル受信入力端子ＲＸＩＮに印加されるシリアル信号を復調しパラレルデータに変換してデータ端子（Ｄ７－Ｄ０）に出力する機能がある。

集積回路３１０のシリアル送信出力端子ＴＸＯＵＴから出力される信号は、信号処理回路３２０を通り、トランス３３０を通って線路ＬｉＢに出力される。また、線路ＬｉＢから入力される信号は、トランス３３０を通り信号処理回路３２０を通って、集積回路３１０のシリアル受信信号入力端子ＲＸＩＮに印加される。集積回路３１０のデータ端子（Ｄ７－Ｄ０）は、データバスＤＢＭ１に接続されている。

第７ｂ図には、モデム４００が示されている。このモデムの回路の大部分は、シングルチップの集積回路４１０で構成されている。この集積回路４１０は上記集積回路３１０と同一のものである。集積回路４１０のシリアル送信出力端子ＴＸＯＵＴから出力される信号は、信号処理回路４２０を通り、トランス４３０を通って線路ＬｉＡに出力される。また、線路ＬｉＡに入力される信号は、トランス４３０を通り、信号処理回路４２０を通って、集積回路４１０のシリアル受信入力端子ＲＸＩＮに印加される。集積回路４１０のデータ端子（Ｄ７－Ｄ０）は、データバスＤＢＭ２に接続されている。

また、第７ａ図に示したモデム３００が出力する割込要求信号ＩＲＱ１と、第７ｂ図に示したモデム４００が出力する割込要求信号ＩＲＱ２との論理和が、論理ゲートＧ１５から出力され、それがマイクロコンピュータ１００の割り込み要求入力端子ＩＮＴに印加される。

第８図に、バッファ回路５００を示す。第８図を参照すると、この回路は、各々双方向スリーステートバスバッファとして機能する、集積回路（７４ＨＣ２４５）５１０，５２０及び５３０で構成されている。集積回路５１０のＡグループの端子はモデム４００のデータバスＤＢＭ２と接続され、集積回路５２０のＡグループの端子はモデム３００のデータバスＤＢＭ１と接続され、集積回路５３０のＡグループの端子はマイクロコンピュータ１００のデータバスと接続されている。また、集積回路５１０，５２０，５３０の各Ｂグループの端子は、内部データバス（２）に共通に接続されている。

従って、集積回路５１０と５３０を制御することにより、マイクロコンピュータ１００のデータバス，内部データバス（２），及びモデム４００のデータバスＤＢＭ２との３者の間で、いずれの方向にもデータを伝送することができ、また集積回路５２０と５３０を制御することにより、マイクロコンピュータ１００のデータバス，内部データバス（２），及びモデム３００のデータバスＤＢＭ１との３者の間で、いずれの方向にもデータを伝送することができる。

第９図には、暗号化／復号化処理回路６００の具体的な構成が示されている。第９図を参照すると、この回路は大きく分けて、鍵コード保持回路６１０，暗号化回路６２０及び復号化回路６３０で構成されている。

まず、鍵コード保持回路６１０を説明する。この回路は、ＰＲＯＭ（プログラマブルＲＯＭ）６１１と２つのラッチ６１２，６１３で構成されている。ＰＲＯＭ６１１のアドレス端子（Ａ０～Ａ７）に、マイクロコンピュータ１００から、マスタ鍵の情報が印加される。ＰＲＯＭ６１１には、各々のアドレスに互いに異なる鍵コードが予めストアしてあり、アドレス情報を与えることにより、そのアドレスに存在する８ビットの鍵コードを、データ端子（Ｄ０～Ｄ７）に出力する。

ラッチ制御信号ＫＬＴ１及びＫＬＴ２を制御することにより、ＰＲＯＭ６１１が出力する情報を、それぞれ、ラッチ６１２及び６１３に保持することができる。ラッチ制御信号ＫＬＴ１を出力する時とＫＬＴ２を出力する時とで、ＰＲＯＭ６１１に与えるマスタ鍵を変えることにより、ラッチ６１２に保持されるデータとラッチ６１３に保持されるデータとが異なる値になる。ラッチ６１２に保持された８ビットデータは、鍵コードＫＡとし

て、ラッチ６１３に保持された８ビットデータは鍵コードＫＢとして、それぞれ、暗号化回路６２０及び復号化回路６３０に印加される。

次に暗号化回路６２０を説明する。この回路は、４ビット全加算器６２１，６２２，排他的論理和（イクスクルーシブオア）回路６２３，６２４，及びスリーステート出力のバッファ６２５で構成されている。全加算器６２１のＡグループの入力端子には、データバスを介して、暗号化すべき情報Ｘの下位４ビットの情報（Ｘ０－Ｘ３）が印加され、Ｂグループの入力端子には、鍵コードＫＡの下位４ビット（Ｋ０－Ｋ３）が印加される。また、全加算器６２２のＡグループの入力端子には、データバスを介して、暗号化すべき情報Ｘの上位４ビット（Ｘ４－Ｘ７）が印加され、Ｂグループの入力端子には、鍵コードＫＡの上位４ビット（Ｋ４－Ｋ７）が印加される。全加算器６２１のキャリー出力は、全加算器６２２の入力端子に印加される。

全加算器６２１及び６２２の各Ｅグループの出力端子は、それぞれ、排他的論理和回路６２３及び６２４のＡグループの入力端子に印加される。また、排他的論理和回路６２３のＢグループの入力端子には鍵コードＫＢの下位４ビット（Ｋ８－Ｋ１１）が印加され、排他的論理和回路６２４のＢグループの入力端子には鍵コードＫＢの上位４ビット（Ｋ１２－Ｋ１５）が印加される。

排他的論理和回路６２３の出力端子Ｙから出力される４ビットの信号及び６２４の出力端子Ｙから出力される４ビットの信号は、バッファ６２５を通って、８ビットの暗号化情報Ｙとして、内部データバス（２）に出力される。

次に復号化回路６３０を説明する。この回路は、４ビット全加算器６３３，６３４，排他的論理和回路６３１，６３２，スリーステート出力のバッファ６３５及びインバータ群で構成されている。排他的論理和回路６３１のＡグループの入力端子には、暗号化された情報Ｙの下位４ビット（Ｙ０－Ｙ３）が、内部データバス（２）から印加され、Ｂグループの入力端子には、鍵コードＫＢの下位４ビット（Ｋ８－Ｋ１１）が印加される。また、排他的論理和回路６３２のＡグループの入力端子には、暗号化された情報Ｙの上位４ビット（Ｙ４－Ｙ７）が、内部データバス（２）から印加され、Ｂグループの入力端子には、鍵コードＫＢの上位４ビット（Ｋ１２－Ｋ１５）が印加される。

排他的論理和回路６３１及び６３２の各Ｅグループの出力端子から出力される信号は、それぞれ、全加算器６３３及び６３４のＢグループの入力端子に印加される。全加算器６３３のＡグループの入力端子には、鍵コードＫＡの下位４ビット（Ｋ０－Ｋ３）を各々反転した信号が印加され、全加算器６３４のＡグループの入力端子には、鍵コードＫＡの上位４ビット（Ｋ４－Ｋ７）を各々反転した信号が印加される。

全加算器６３３が出力する４ビットの情報と全加算器６３４が出力する４ビットの情報は、バッファ６３５を介して、復号化された８ビットの情報Ｘとして、マイクロコンピュータ１００のデータバスに出力される。

なお、上記暗号化回路６２０及び復号化回路６３０が行なう暗号処理の方法は、基本的には従来より知られているものであるので、それに関する説明は不要であろう。なお、第９図に示した暗号化／復号化処理回路６００の処理の内容を簡略化したものを第４図に示すので参照されたい。

第１０図に、この実施例で用いたメモリカード１３０の内部構造を示す。第１０図を参照すると、このメモリカードには、読み書きメモリ（ＲＡＭ），バッテリー，制御回路及びコネクタ１３４が備わっており、コネクタ１３４によって、秘匿装置の本体に対し着脱自在になっている。コネクタ１３４の各端子には、電源ライン（Ｖcc），カードセット信号端子（ＣＳＴ），チップセレクト信号端子（ＣＳ），書き込み制御出力（ＷＰＯＵＴ），書込制御入力（ＷＥ），出力許可入力（ＯＥ），アドレスバス（Ａ０－Ａ１２）及びデータバス（Ｄ０－Ｄ７）が割当てられている。ＲＡＭ１３１に、このメモリカード固有の（予め割当てられた）ＩＤコードが書込まれている。この実施例で

は、秘匿通信を行なうためには、同一のＩＤコードが書込まれたメモリカードが、送信側と受信側の双方の秘匿装置に必要である。

次に、実際の通信動作について説明する。通信を行なうファクシミリ装置の動作を、第１１ａ図，第１１ｂ図，第１１ｃ図，第１１ｄ図，第１１ｅ図，第１１ｆ図及び第１１ｇ図に示し、秘匿装置の動作を第１２ａ図，第１２ｂ図，第１２ｃ図，第１２ｄ図，第１２ｅ図，第１２ｆ図，第１２ｇ図，第１２ｈ図，第１２ｉ図，第１２ｊ図及び第１２ｋ図に示す。なお、ファクシミリ装置自体の処理の内容は、従来の装置と同一であるので、その部分については簡単に説明する。

以下、各図を参照して処理の内容を説明するが、その説明においては、第１図に示されるように、通信系が構成されているものとする。また、以下の説明においては、通信処理で伝送する信号の記号（括弧内に示す）には、ＣＣＩＴＴの勧告によって定められた略号を用いてある。更に、ファクシミリは発呼側も被呼側も自動モードで動作するものとして説明する。

発呼側のファクシミリでは、フックをオフし（受話器を上げる動作に相当する）、交換機からのダイアルトーンを検出すると、相手局の番号をダイアルする（第１１ａ図参照）。

被呼側では、交換機からの呼び出し音（リング音）を検出すると、フックをオフし、続いてそれがファクシミリであることを示す被呼局識別信号（ＣＥＤ）を回線に送出する。発呼側では、この信号（ＣＥＤ）を検出するまで、発呼側がファクシミリであることを示す発呼トーン（ＣＮＧ）を回線に送出し続ける。

発呼側では、信号（ＣＥＤ）を検出後、ファクシミリの通信モードに入る。被呼側では、信号（ＣＥＤ）を送出後、被呼装置がＣＣＩＴＴの標準能力を有することを示す、デジタル識別信号（ＤＩＳ）を送出する。つまり、信号（ＤＩＳ）によって被呼側のファクシミリがどのモードの（Ｇ１，Ｇ２，Ｇ３等）通信能力があるかを発呼側に知らせる。

発呼側では、被呼側から送信されたデジタル識別信号（ＤＩＳ）の内容から、自局ファクシミリの通信能力と合うかどうかをチェックし、双方の通信能力に合った通信モードを決定し、ＤＩＳ信号に応答するデジタル命令信号（ＤＣＳ）を被呼側に返送する。それに続いて、回線の状態をチェックする為にトレーニングチェック信号（ＴＣＦ）を送信する。被呼側では、信号（ＤＣＳ）を受けた後、指定されたモードで信号（ＴＣＦ）を受信し、その受信結果を示す信号（ＣＦＲ又はＦＴＴ）を返送する。

発呼側では、返送された受信結果により、通信状態が良好なら、次のメッセージ送信ステップに移り、状態が悪ければ通信モードを変更して（一般には通信速度を下げて）、再度信号（ＴＣＦ）を送出する。

発呼側で信号（ＣＦＲ）を受信すると、トレーニング信号を送出し、被呼側に同期をとらせ、続いてメッセージを送信する。被呼側では、トレーニング信号で同期をとった後、メッセージを受信する。

被呼側では、発呼側が１頁の原稿を送信後、その終りを示すために送出する信号（ＲＴＣ）を検出するまで、受信を続ける。

１頁の原稿を送信すると、発呼側では、最終原稿かどうかを検出し、最終原稿でなければ、マルチページ信号（ＭＰＳ）を送った後、受信側から送出される受信確認信号（ＭＣＦ）又は再トレーニング信号（ＲＴＰ，ＲＴＮ）を受信する。そして、受信した信号により、送信モードを変更するか、トレーニング送出か、又は回線切断かを選択する。

最終原稿である場合、割り込みによる手順の中断が入り、モード変更するか否かを識別し、モード変更しない場合には、手順終了信号（ＥＯＰ）を送出後、回路切断動作に入る。モード変更する場合には、信号（ＭＣＦ，ＲＴＰ，ＲＴＮのいずれか）を受信すると、デジタル識別信号（ＤＩＳ）を受信するまで待つ。

被呼側では、発呼側からの信号（ＭＰＳ），

（ＥＯＰ），（ＥＯＭ：メッセージ終了）のいずれかを受信すると、信号（ＭＣＦ），（ＲＴＰ），（ＲＴＮ）のいずれかで応答した後、命令受信状態に戻る。それ以外は回路切断動作に入る。

次に、秘匿装置の動作を説明する。

まず最初に、自局のファクシミリが発呼側と被呼側のいずれに属するかを識別する。つまり、第１２ａ図において、ステップＡ５２で、呼び出し検出回路２２０の出力する（着呼）信号をチェックし、ステップＡ５５で、極性検出回路２１０の出力するフック信号をチェックし、着呼検出とフックオフ検出のいずれか先かを識別することによって、発呼側か被呼側かを検出する。被呼側であれば、まず最初に着呼信号が検出されるので、ステップＡ５３でレジスタC_1に１をストアする。発呼側であれば、着呼信号が検出されない時にステップＡ５４でレジスタC_1に０をストアし、フックオフが検出されるので、次の処理に進む。従って、以降の処理では、レジスタC_1を参照することによって、自局のファクシミリが発呼側か被呼側かを識別できる。

次に、秘匿装置にメモリカード１３０が装着されたか否かを識別する。これは、メモリカード１３０から出力されるカード装着信号ＣＳＴを参照することによって識別できる。発呼側と被呼側の少なくとも一方の秘匿装置にメモリカード１３０が装着されると、それによって秘匿通信の意志があるものとみなす。

メモリカード１３０が装着されると、ステップＡ５９に進んでリレーＲＹ１をオンし、ステップＡ６０でレジスタC_1の値をチェックし、発呼側又は被呼側の処理を行なう。

自局が被呼側の場合、ステップＡ６９で、スイッチ（ＦＡＸ－ＳＷ：ＳＷ１）をチェックし、自局のファクシミリのモードが手動か自動かを識別する。手動なら、ステップＡ７０に進み、リレーＲＹ２をオンにして、自局ファクシミリの回線ＬＦ１，ＬＦ２を秘匿装置内の線路ＬｉＢに接続し、ステップＡ７１で、相手側、即ち発呼側の局に信号（ＣＥＤ）を送出する。

自局のファクシミリが自動モードなら、第１２ｇ図のステップＧ５１に進む。そして、自局のファクシミリからの信号（ＣＥＤ）を検出すると、所定時間T_{x2}後に、リレーＲＹ２をオンし、自局ファクシミリの回線ＬＦ１，ＬＦ２を秘匿装置内の線路ＬｉＢに接続する。

次に、秘匿スイッチ（ＳＷ２）の状態をチェックする。スイッチがオンなら、秘匿希望有とみなし、レジスタＭｒにＡＣＴＣをストアし、そうでなければ、ＭｒにＮＡＣＴＣをストアする。次に、ステップＧ６１に進み、信号（ＤＩＳ）が受信可能な状態に設定する。

次に、第１２ｈ図のステップＨ５１に進み、レジスタＭｒの内容を、相手局に送出する。

ここで、自局が発呼側の場合を説明する。その場合、第１２ｂ図に示すステップＢ５１に進み、まず信号（ＣＥＤ）を検出するまで待つ。この信号（ＣＥＤ）を検出すると、次にステップＢ５６に進む。被呼側の局が通常のファクシミリであると、ここでＤＩＳ又はＤＴＣが送られるが、被呼側の局の秘匿装置が動作していると信号（ＣＥＤ）に続く、ＤＩＳ又はＤＴＣのかわりに、第１２ｈ図のステップＨ５１で、Ｍｒの内容が送られる。その場合、所定時間T_{x2}を経過すると、ステップＢ５７からステップＢ５８に進み、リレーＲＹ２をオンして回線の接続を切換え、ステップＢ５９で秘匿スイッチ（ＳＷ２）の状態を識別し、その結果に応じてレジスタＭｔの内容を設定する。そして、レジスタＭｒの内容が受信されるので、ステップＢ６６から、第１２ｃ図のステップＣ５１に進む。そして、レジスタＭｒとＭｔのいずれかがＡＣＴＣ、即ち秘匿希望であると、ステップＣ５５に進む。

ステップＣ５５では、乱数発生回路が出力する信号ＲＤＭのレベルを繰り返しサンプリングし、それによって乱数コードＲを生成する。ステップＣ５６では、生成された乱数コードＲを、暗号化／復号化処理回路６００の入力Ｘとして与えるとともに、メモリカード１３０から得たＩＤコードをマスタ鍵として暗号化／復号化処理回路６００

に与え、該マスタ鍵に対応する鍵コードＫＡ及びＫＢを生成し、乱数Ｒを暗号化した情報Ｃｔを生成する。次のステップＣ５７では、コードＡＣＴＣに暗号Ｃｔを付加した情報Ｘｔを、被呼側の局に送出する。

被呼側の局では、第１２ｂ図のステップＨ５２で、発呼局からの情報Ｘｔを受信する。そして、ＸｔがＮＡＣＴＣでなければ、ステップＨ５６に進む。ステップＨ５６では、被呼局のメモリカード１３０から得たＩＤコードをマスタ鍵として暗号化／復号化処理回路６００に与え、該マスタ鍵に対応する鍵コードＫＡ及びＫＢを生成する。そして、受信した暗号を暗号化／復号化処理回路６００の暗号入力Ｙに与え、その暗号を解読する。解読した情報Ｒ'は、データバスに出力される。次のステップＨ５７では、今度は解読した情報Ｒ'を、マスタ鍵として、暗号化／復号化処理回路６００に与え、該マスタ鍵に対応する鍵コードＫＡ，ＫＢを生成する。そして、情報Ｒ'を暗号化／復号化処理回路６００に入力情報Ｘとして入力し、それを暗号化し、得られた暗号Ｘｒを、発呼側の局に送出する。

発呼側の局では、ステップＣ５８で暗号Ｘｒを受信すると、ステップＣ５９に進む。ステップＣ５９では、暗号Ｘｒを、暗号化／復号化処理回路６００の暗号入力Ｙに入力するとともに、最初に送った乱数と同一の値をマスタ鍵として暗号化／復号化処理回路６００に与え、暗号Ｘｒを復号化する。このようにして復号化される情報Ｒ''は、

$$R'' = Dr(Er'(R')) \quad \cdots(1)$$

但し、Ｒ'：被呼側が解読したＲ

Ｅｒ'：被呼側の暗号化の関数

Ｄｒ：発呼側の復号の関数

であるから、発呼側と被呼側の暗号化及び復号化の条件が全て一致する場合には、Ｒ''は最初に送った乱数Ｒと等しくなる。もし、初呼側のメモリカードと被呼側のメモリカードに記憶されたＩＤコードが異なる場合には、ＲとＲ''とは一致しない。発呼局側はステップＣ６０でＲとＲ''とを比較し、それが一致すると、ステップＣ６２に進み、レジスタＲｆに１をストアしてそれを被呼側に送出する。もし一致しない場合には、暗号の送出と返送される暗号との照合が３回繰り返される。３回の照合で一致しなければ、秘匿通信の動作は禁止される。

被呼側では、第１２ｈ図のステップＨ５８で、Ｒｆを受信すると、ステップＨ６１以降の処理に進む。

上述のようにして秘匿通信が可能な状態になるまでの間は、被呼局側のファクシミリは、デジタル識別信号（ＤＩＳ）を送出し続けており、発呼側のファクシミリはその信号を待ち続けている。そして、被呼局側の秘匿装置は、ステップＨ６５に進むと、既に自局ファクシミリからのデジタル識別信号（ＤＩＳ）を受信しているので、その信号を相手側（発呼側）の局に送信する。

このようにして秘匿通信が可能な状態になると、後は通常のファクシミリ通信と同様の手順で情報の伝送が行なわれるが、その場合、秘匿装置は自局側のファクシミリと相手局側（秘匿装置）とのデータ伝送の仲介を行なうことになり、自局側のファクシミリが送信した情報は、秘匿装置を介して相手局に送られ、相手局から送られた情報は、秘匿装置を介して自局のファクシミリに送られる。画像情報に対しては、仲介する際に、暗号化又は復号化が行なわれる。その場合、暗号化すべき情報は、暗号化／復号化処理回路６００の入力端子Ｘに印加され、復号化すべき情報は入力端子Ｙに印加される。また、暗号化／復号化処理回路６００のマスタ鍵コードとしては、自局と相手局との間で既に転送され確認及び照合された、乱数がいずれの局においても使用される。つまり、秘匿通信で使用される鍵、即ち、セッション鍵には、通信の度に互いに異なる値が使用される。従って、極めて安全性が高い。

なお、上記実施例においては、算術加算と排他的論理和の演算によって暗号化／復号化を行なっているが、暗号化の方式に関しては、従来より知られる他の様々な方法を用いても本発明は同様に実施しうる。例えば、ストリーム暗号のように、

鍵の値をカウントアップするなどの方法により逐次更新する方法を用いてもよいし、暗号化した直前のデータを鍵として利用する方法を用いてもよい。

また、実施例では、ファクシミリ同志で通信を行なう場合の秘匿通信について説明したが、同様の通信手順で通信を行なう装置であれば、ファクシミリに限らず、本発明の装置を用いて、秘匿通信を行なうことが可能である。

[効果]

以上のとおり、本発明によれば、ファクシミリの通信プロトコルにおいて、ＣＣＩＴＴによって規定されたフェーズＡからフェーズＢに移行する前に、切換スイッチ手段によって、通信回線（第１組の信号線：ＬＮ１，ＬＮ２）から自局側通信手段が切離され、その状態で通信回線に接続された秘匿通信制御装置同志の間で、鍵に関する情報のやりとりが行なわれる。従ってこの場合には、鍵に関する情報の受渡しを、実質上何回でも行なうことが可能である。このため、伝送路上における情報の変形などによって、鍵の情報の受渡しが失敗した場合、その受渡しのやり直しを、回線を切断することなく実行することができる。この情報の受渡しの際には、自局側及び相手側の通信手段（ファクシミリ）は、フェーズＢに移行する前の待機状態であり、格別な不都合は生じない。

鍵の受渡しが完了した後は、その鍵に基づいて秘匿通信制御装置が、メッセージ情報の暗号化又は解読を行ないながらそれの中継を行なうことにより、秘匿通信を行なうことができる。

4．図面の簡単な説明

第１図は、実施例の秘匿装置を利用する通信系全体の構成を示すブロック図である。

第２図は、送信側と受信側に各々設けられた秘匿装置の構成の概要を示すブロック図である。

第３図は、実施例の１つの秘匿装置の構成を示すブロック図である。

第４図は、暗号化／復号化処理回路６００の機能の概略を示すブロック図である。

第５ａ図，第５ｂ図，第５ｃ図，第５ｄ図，第６ａ図，第６ｂ図，第７ａ図，第７ｂ図，第８図，第９図及び第１０図は、第４図に示す各部の詳細構成を示すブロック図である。

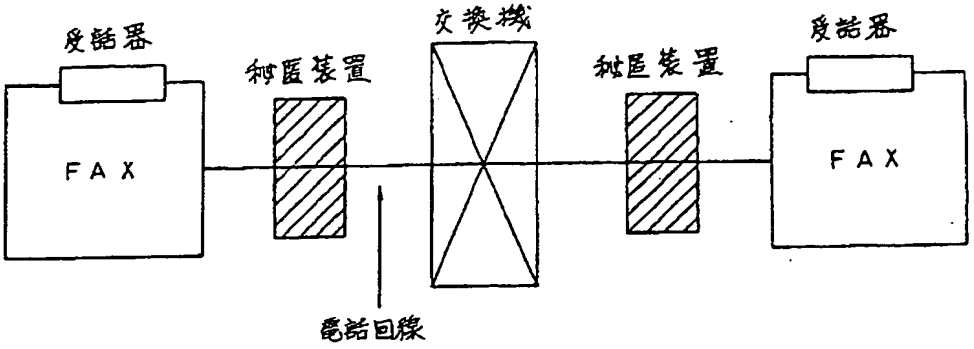
第１１ａ図，第１１ｂ図，第１１ｃ図，第１１ｄ図，第１１ｅ図，第１１ｆ図及び第１１ｇ図は、ファクシミリの通信処理の内容を示すフローチャートである。

第１２ａ図，第１２ｂ図，第１２ｃ図，第１２ｄ図，第１２ｅ図，第１２ｆ図，第１２ｇ図，第１２ｈ図，第１２ｉ図，第１２ｊ図及び第１２ｋ図は、秘匿装置の動作を示すフローチャートである。

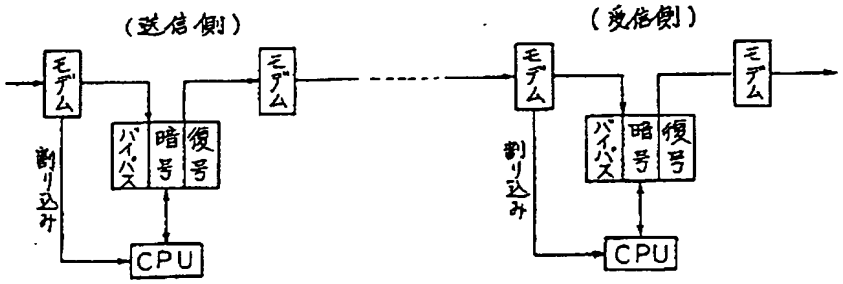
１００：マイクロコンピュータ（電子制御手段）
１１０：ROM　１２０：RAM
１３０：メモリカード　１３４：コネクタ
１４０：電源　１５０：乱数発生回路
１８０：入出力インターフェース
２１０：極性反転検出回路　２２０：呼び出し検出回路
２３０：電流供給回路
３００：モデム（第２の変復調手段）
３１０，４１０：集積回路　３２０，４２０：信号処理回路
３３０，４３０：トランス　400：モデム(第１の変復調手段)
５００：バッファ回路
６００：暗号化／復号化処理回路(秘匿情報処理手段)
６１０：鍵コード保持回路　６１１：PROM
６１２，６１３：ラッチ　６２０：暗号化回路
６２１，６２２：全加算器　623，624：排他的論理和回路
６２５：バッファ　６３０：復号化回路
631，632：排他的論理和回路　６３３，６３４：全加算器
６３５：バッファ　RY1：リレー
RY2：リレー（切換スイッチ手段）
LN1，LN2：公衆電話回線(第１組の信号線)
LF1，LF2：回線（第２組の信号線）
LiA：線路　LiB：線路（第３組の信号線）
LT1：ラッチ　DE1，DE2：デコーダ
SW1－SW6：スイッチ　LED1－LED7：発光ダイオード
BZ：ブザー　PC1，PC2：フォトカップラ

出願人　アイシン精機株式会社
代理人　弁理士　杉信興

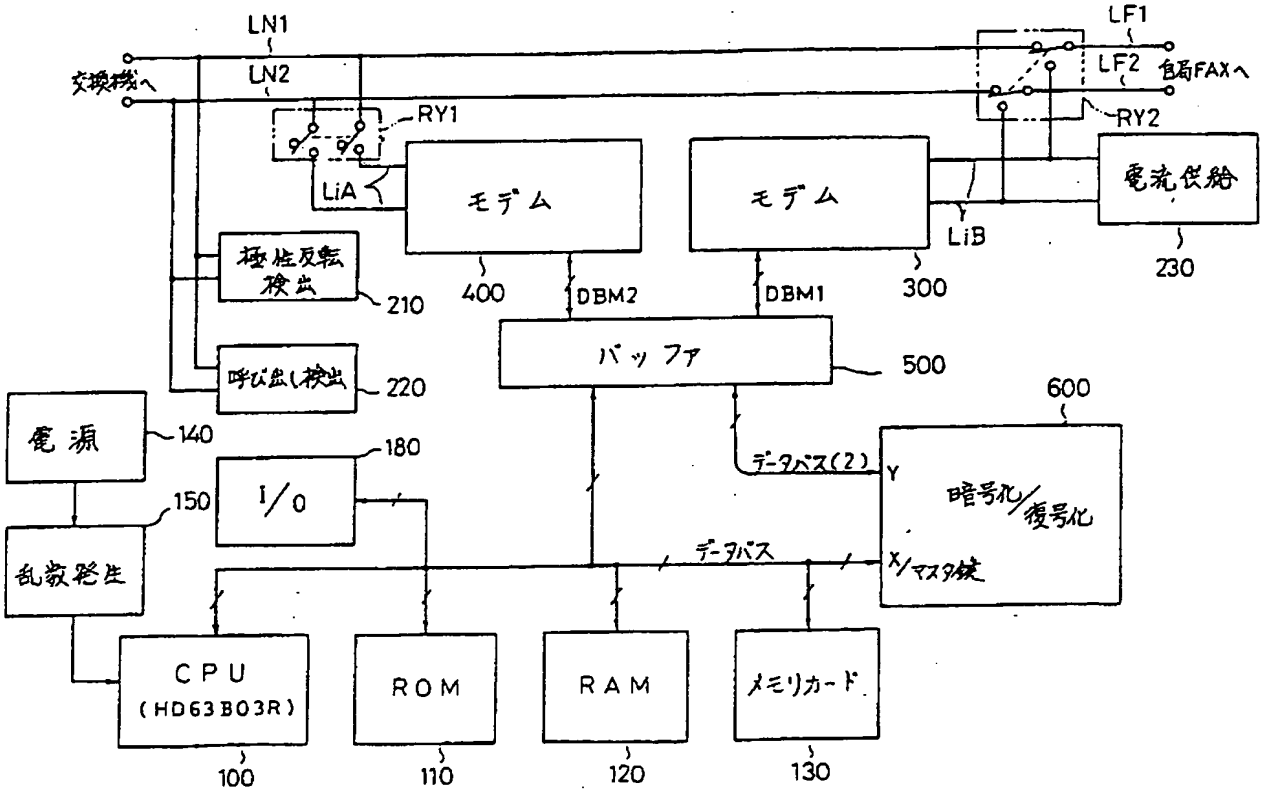
第 1 図


受話器
秘匿装置
交換機
秘匿装置
受話器
FAX
FAX
電話回線

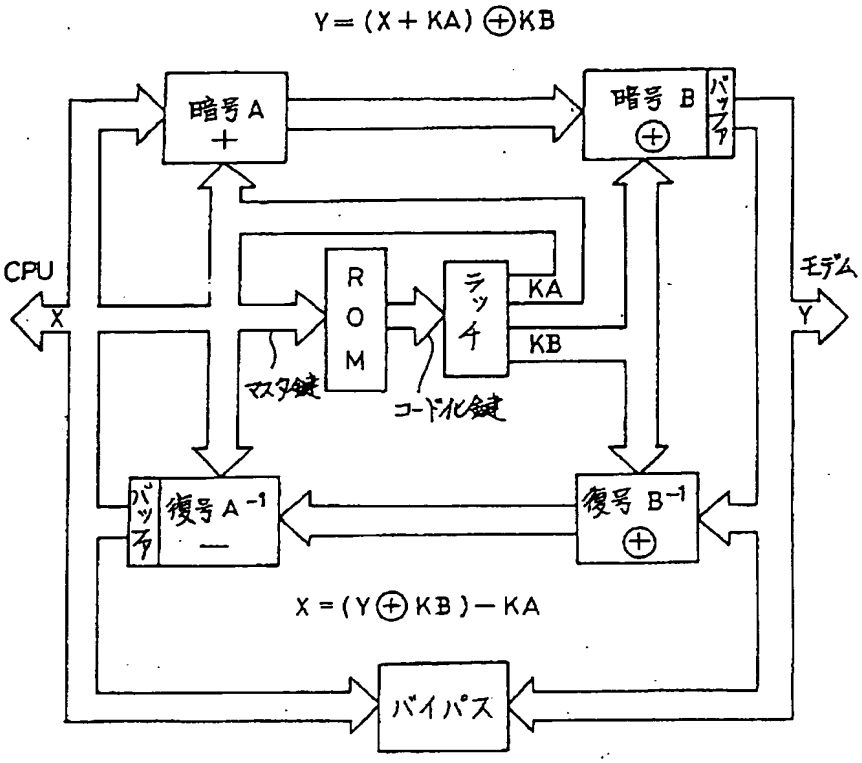
第 2 図


(送信側)
(受信側)
モデム
モデム
モデム
モデム
バイパス
暗号
復号
バイパス
暗号
復号
割り込み
割り込み
CPU
CPU

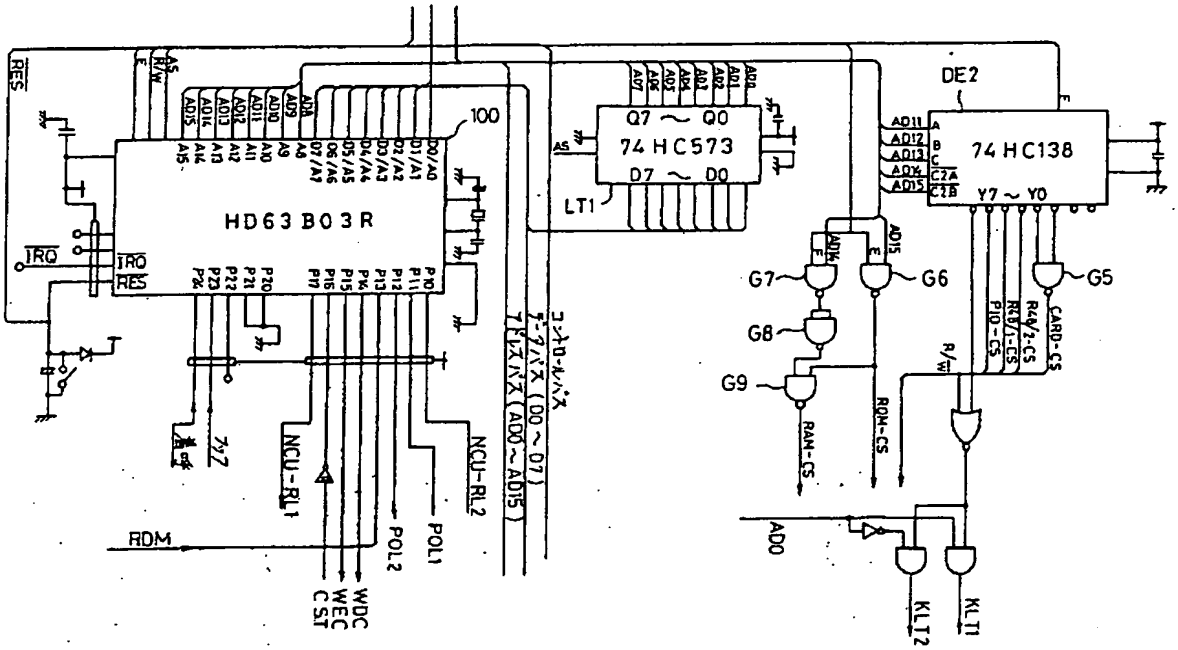
第 3 図


LN1
LN2
交換機へ
LF1
LF2
自局FAXへ
RY1
RY2
LiA
LiB
モデム
モデム
電流供給
極性反転検出
210
400
DBM2
DBM1
300
230
バッファ
500
呼び出し検出
220
600
電源
140
180
I/O
150
データバス(2)
Y
暗号化/復号化
乱数発生
データバス
X/マスタ鍵
CPU
(HD63B03R)
ROM
RAM
メモリカード
100
110
120
130

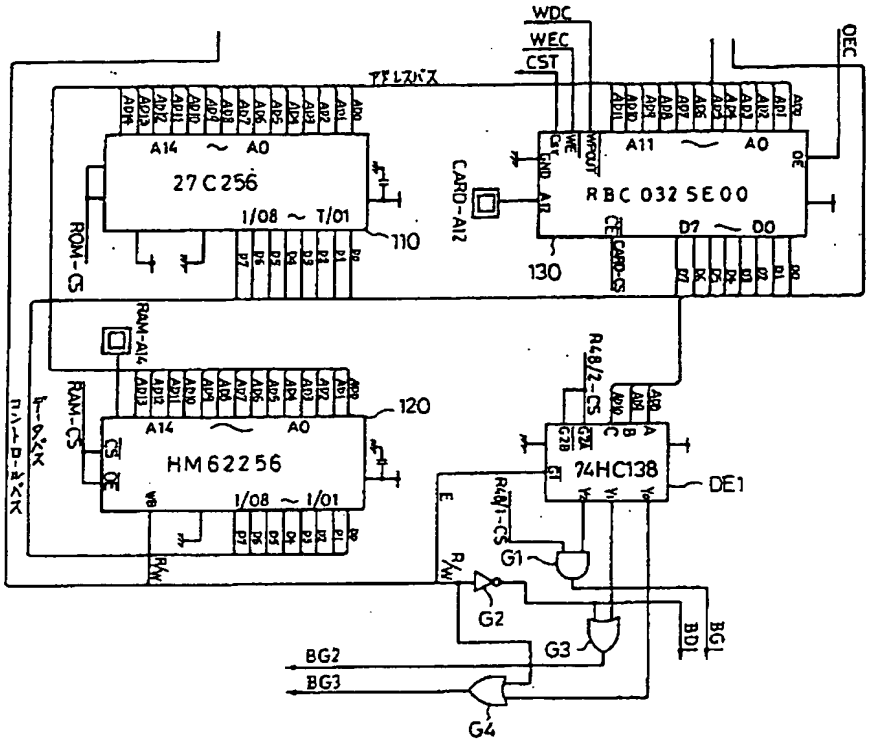
第 4 図


Y=(X+KA)⊕KB
暗号A
+
暗号B
⊕
バッファ
CPU
X
ROM
ラッチ
KA
KB
モデム
Y
マスタ鍵
コード化鍵
バッファ
復号A⁻¹
−
復号B⁻¹
⊕
X=(Y⊕KB)−KA
バイパス

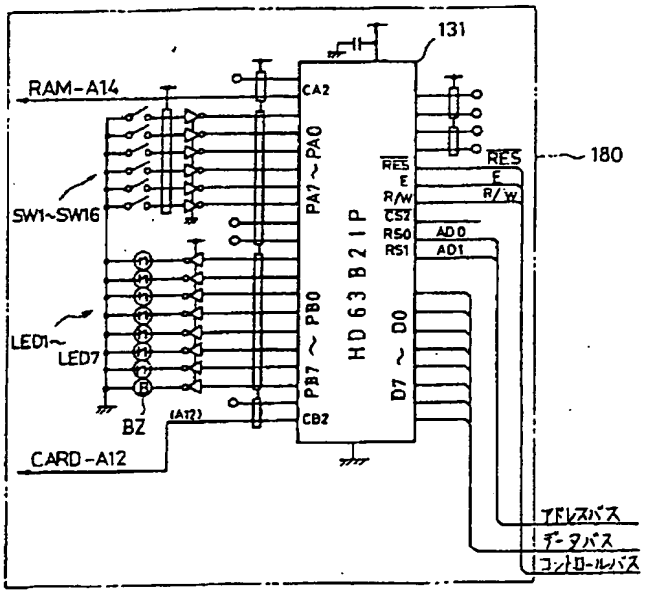
第 5a 図


HD63B03R
74HC573
Q7 ～ Q0
D7 ～ D0
LT1
74HC138
Y7 ～ Y0
DE2
G5
G6
G7
G8
G9
RAM-CS
ROM-CS
CARD-CS
R/W
AD0
KLT1
KLT2
RDM
NCU-RL1
NCU-RL2
POL1
POL2
WDC
WEC
CST
IRQ
RES
100

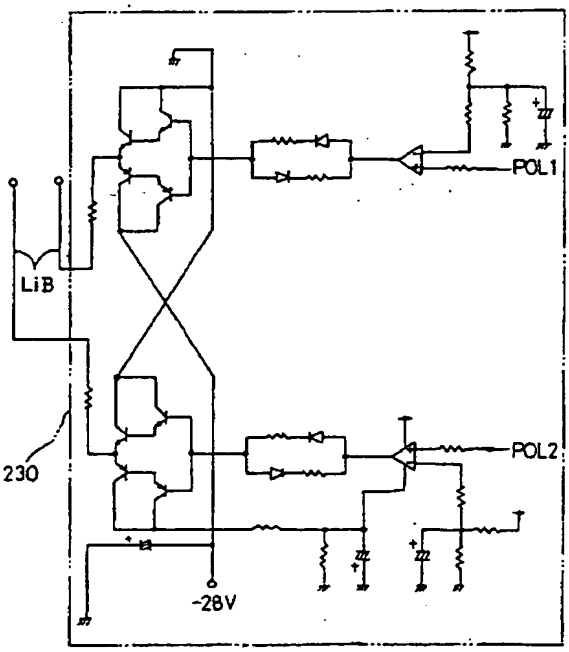
第 5b 図



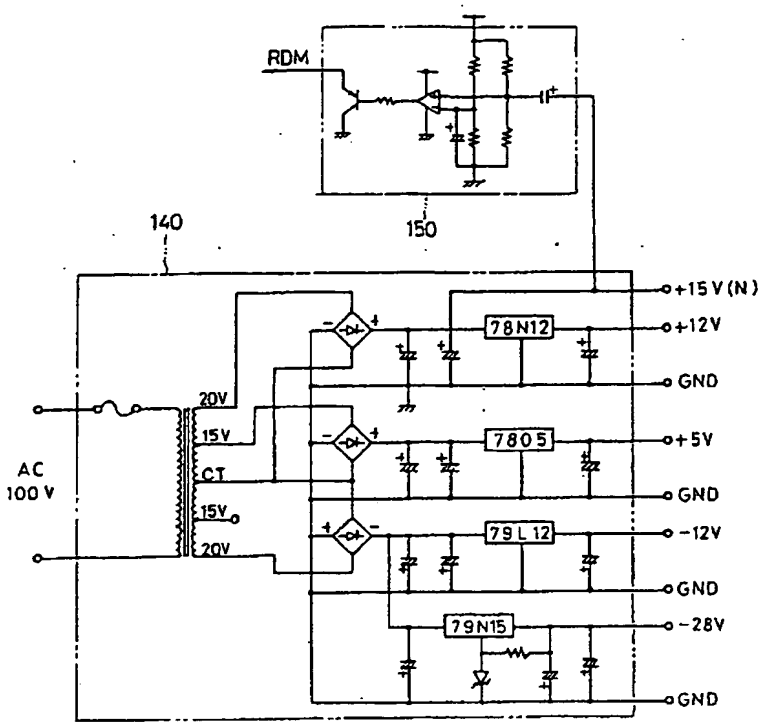
第 5c 図



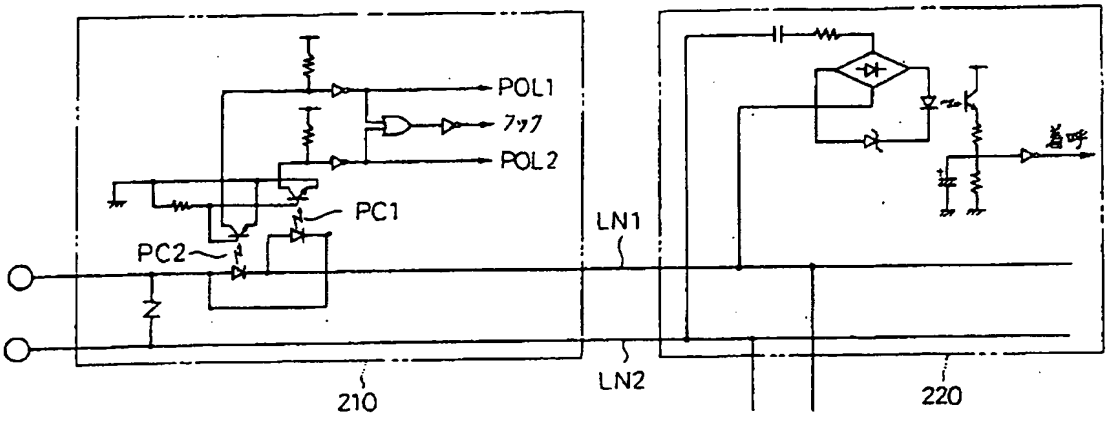
第 6b 図

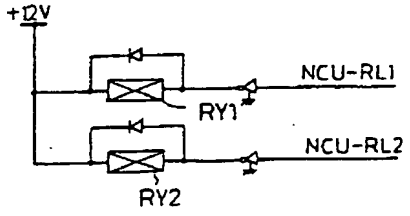


第5d図

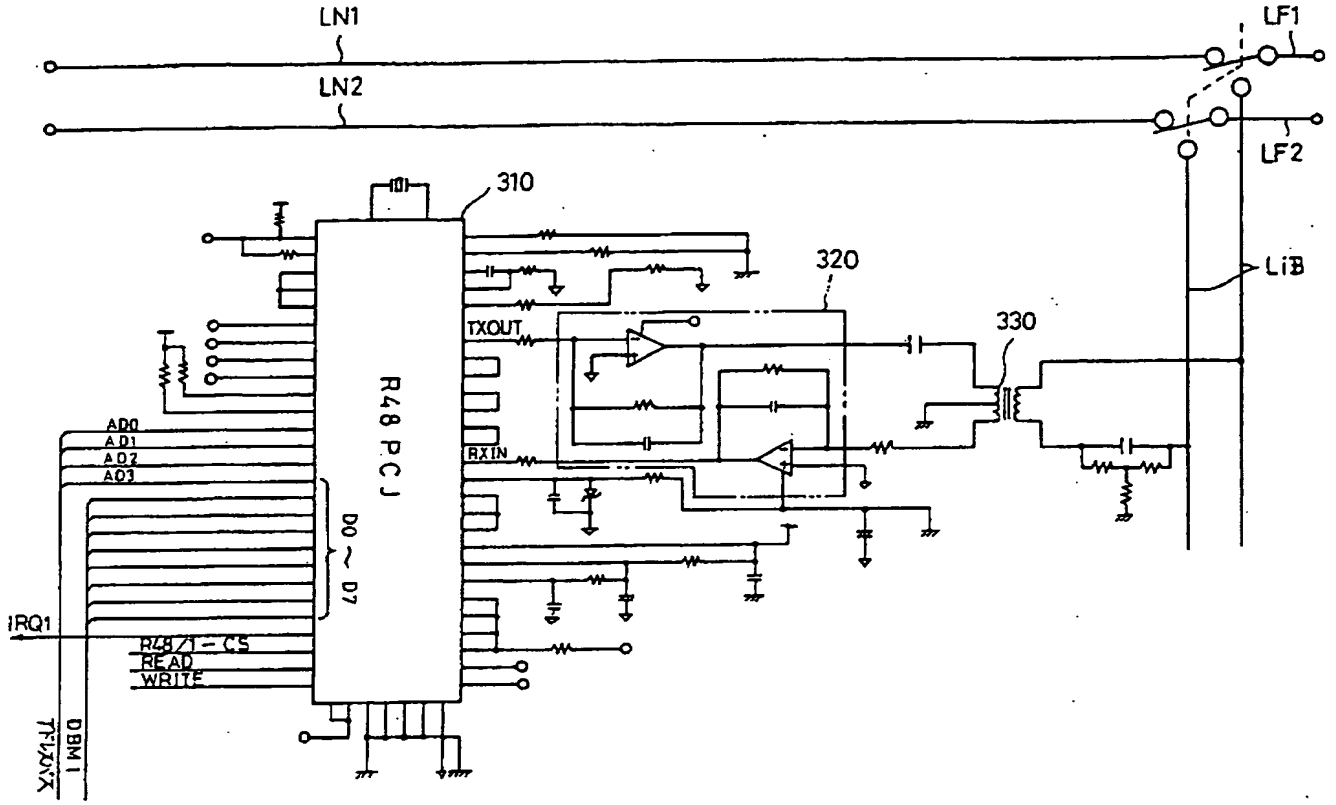

RDM
140
150
+15V(N)
78N12
+12V
GND
20V
15V
CT
15V
20V
AC
100V
7805
+5V
GND
79L12
-12V
GND
79N15
-28V
GND

第6a図

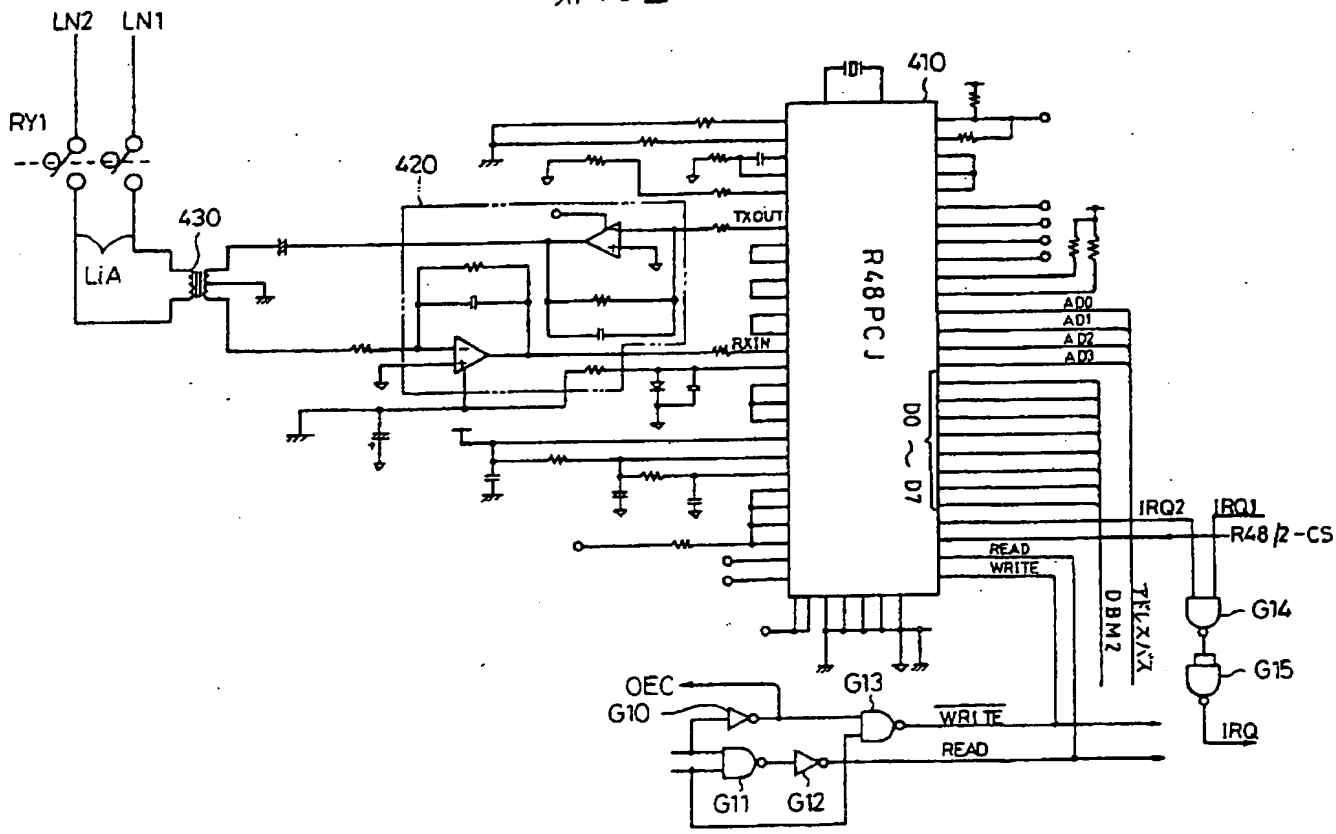

POL1
フック
POL2
PC1
PC2
LN1
LN2
着呼
210
220


+12V
NCU-RL1
RY1
NCU-RL2
RY2

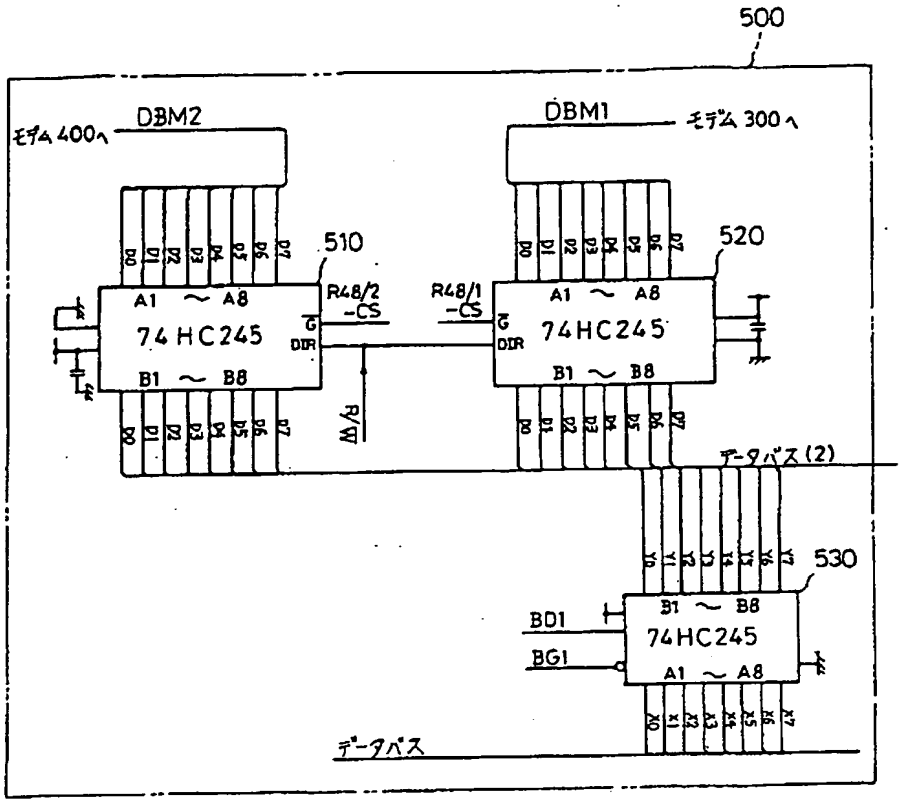
第 7a 図


LN1
LN2
LF1
LF2
LiB
310
320
330
TXOUT
RXIN
R48PCJ
AD0
AD1
AD2
AD3
D0 ~ D7
IRQ1
R48/1-CS
READ
WRITE
DBM1
TXJYX

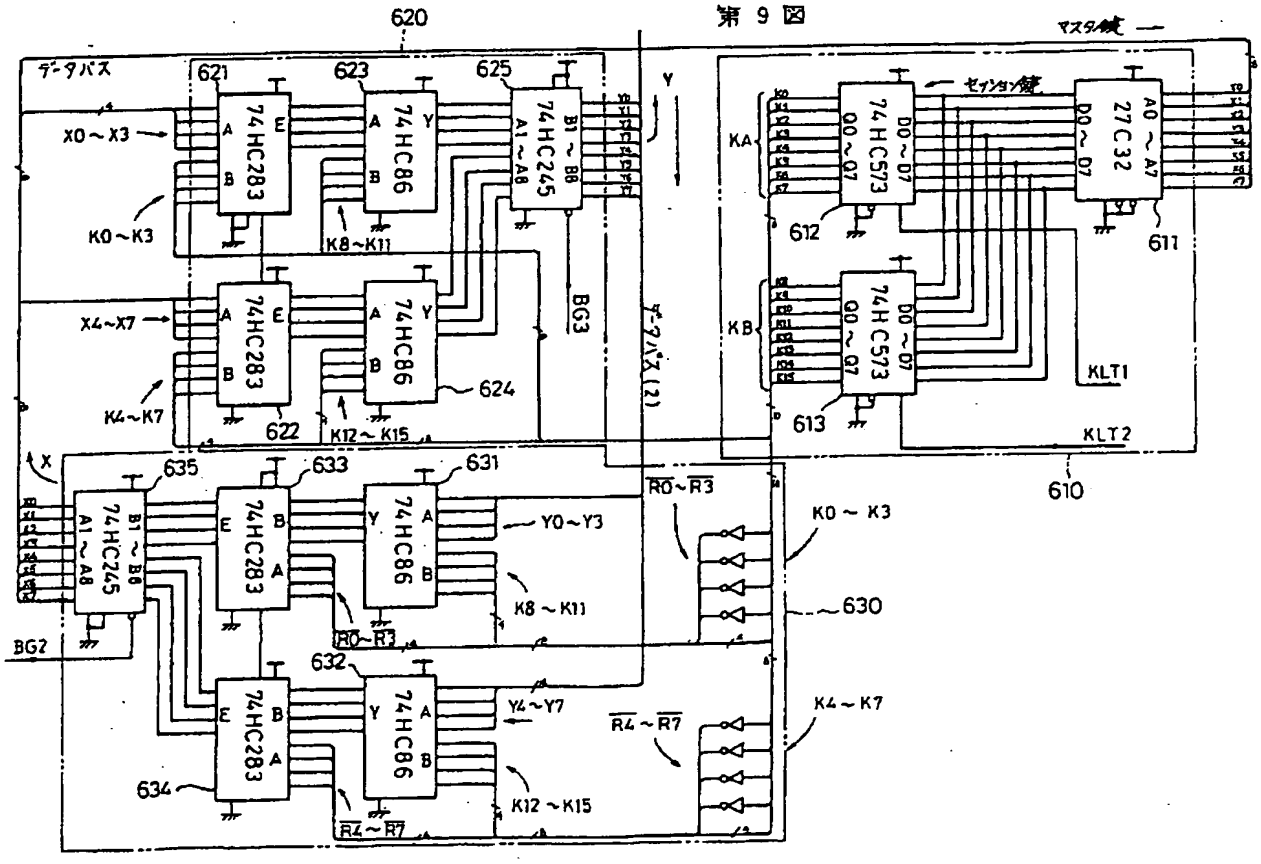
第 7b 図


LN2
LN1
RY1
LiA
410
420
430
TXOUT
RXIN
R48PCJ
AD0
AD1
AD2
AD3
D0 ~ D7
IRQ2
IRQ1
R48/2-CS
READ
WRITE
DBM2
TXJYX
G14
G15
IRQ
OEC
G10
G13
G11
G12
WRITE
READ

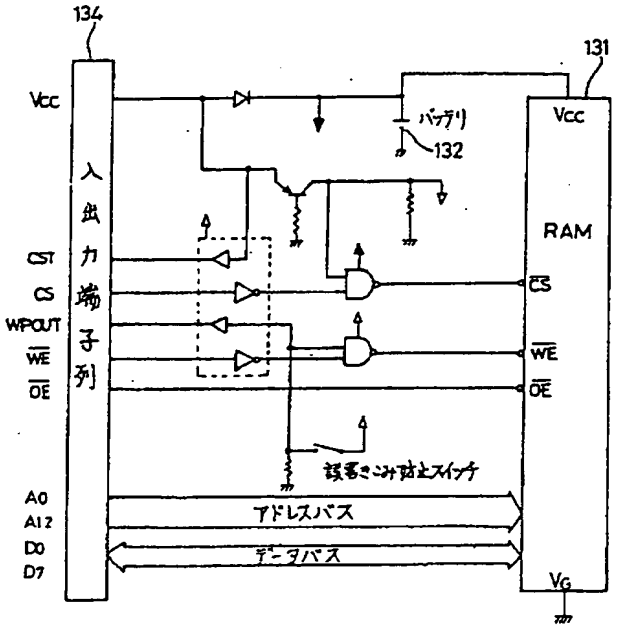
第 8 図


500
DBM2
モデム 400へ
DBM1
モデム 300へ
510
520
530
74HC245
R48/2 -CS
R48/1 -CS
R/W
データバス(2)
BD1
BG1
データバス

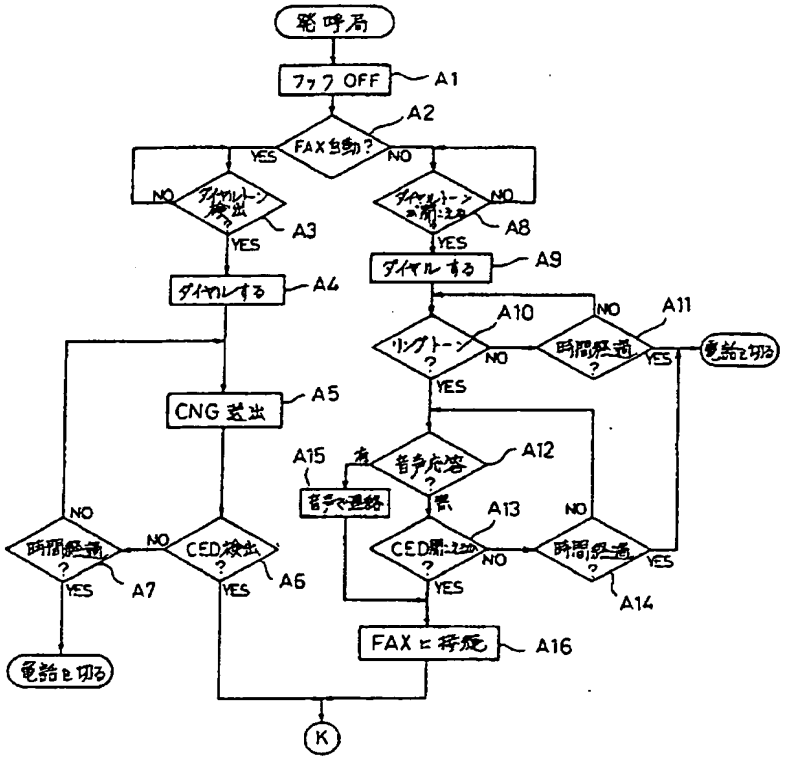
第 9 図


620
データバス
621
623
625
74HC283
74HC86
74HC245
X0～X3
K0～K3
K8～K11
X4～X7
K4～K7
K12～K15
622
624
BG3
データバス(2)
Y
マスタ鍵
セッション鍵
KA
KB
74HC573
27C32
612
613
611
KLT1
KLT2
610
X
635
633
631
632
634
BG2
R0～R3
Y0～Y3
Y4～Y7
R4～R7
630

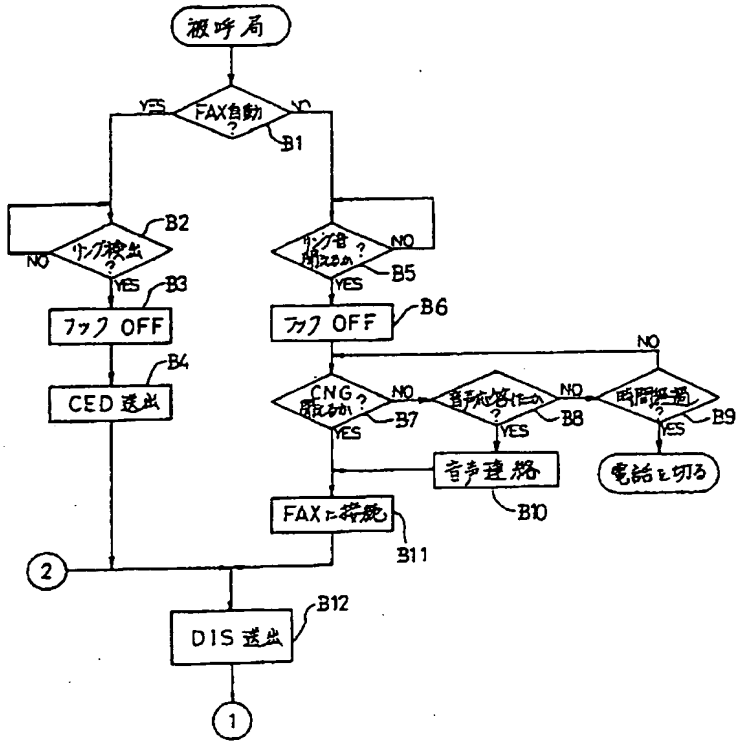
第 10 図


134
131
Vcc
入出力端子列
バッテリ
132
Vcc
RAM
CST
CS
WPOUT
WE
OE
CS
WE
OE
誤書きこみ防止スイッチ
A0
A12
D0
D7
アドレスバス
データバス
VG

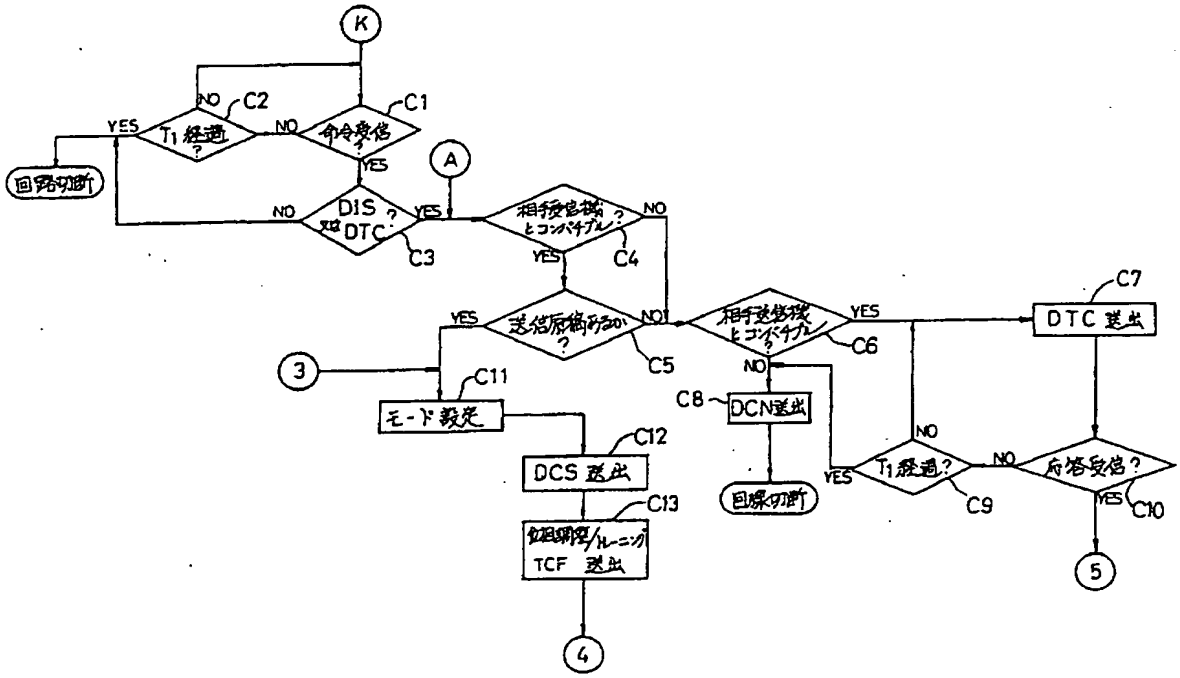
第 11a 図


発呼局
フック OFF
A1
FAX自動?
A2
YES
NO
ダイヤルトーン検出?
A3
NO
YES
ダイヤルする
A4
CNG 送出
A5
CED検出?
A6
NO
YES
時間経過?
A7
NO
YES
電話を切る
ダイヤルトーン検出?
A8
NO
YES
ダイヤルする
A9
リングトーン?
A10
NO
YES
時間経過?
A11
NO
YES
通話を切る
音声応答?
A12
有
無
A15
音声で通信
CED検出?
A13
NO
YES
時間経過?
A14
NO
YES
FAXに移行
A16
K

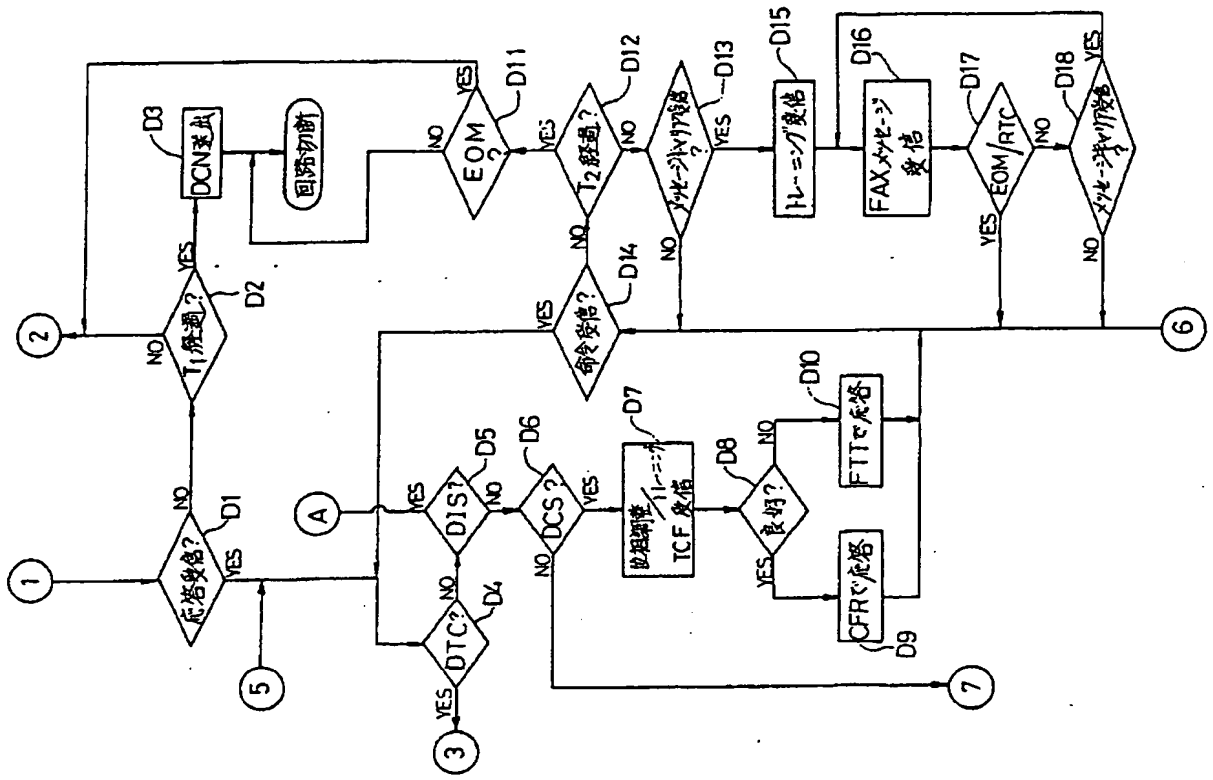
第 11b 図


被呼局
FAX自動?
YES
NO
B1
リング検出?
NO
YES
B2
フック OFF
B3
CED 送出
B4
リング音 消えるまで?
NO
YES
B5
フック OFF
B6
CNG 検出か?
NO
YES
B7
音声応答にするか?
NO
YES
B8
時間経過?
NO
YES
B9
音声連絡
B10
電話を切る
FAXに接続
B11
2
DIS 送出
B12
1

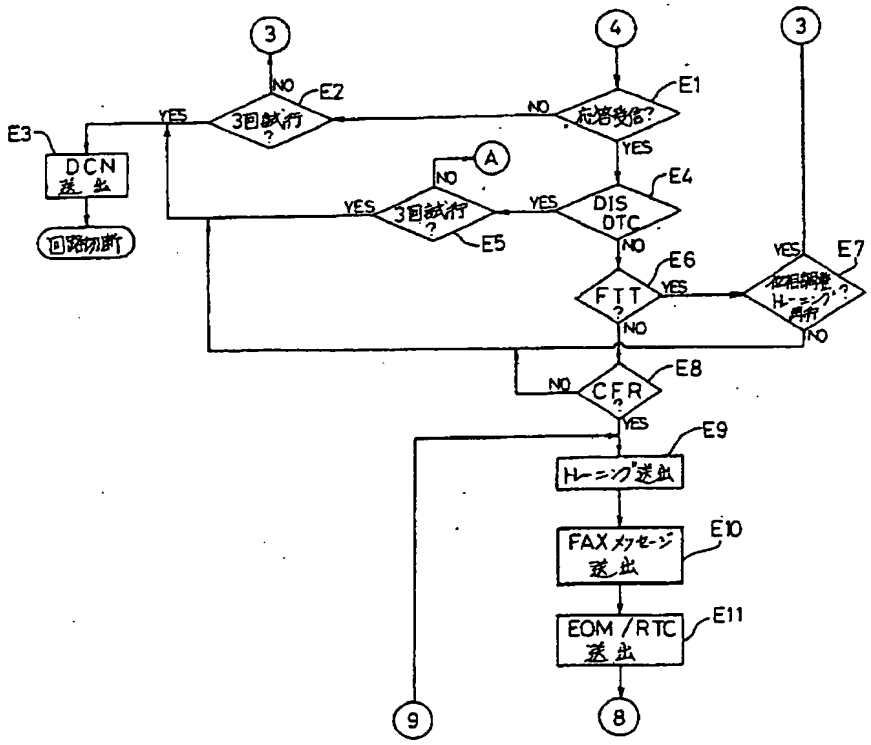
第 11c 図


K
T1 経過?
YES
NO
C2
命令受信?
NO
YES
C1
回線切断
A
DIS 受信 DTC?
NO
YES
C3
相手受信機とコンパチブル?
NO
YES
C4
送信原稿があるか?
YES
NO
C5
相手受信後とコンパチブル?
YES
NO
C6
DTC 送出
C7
3
C11
モード設定
C8
DCN送出
C12
DCS 送出
回線切断
C13
位相調整/トレーニング TCF 送出
T1 経過?
NO
YES
C9
応答受信?
NO
YES
C10
4
5

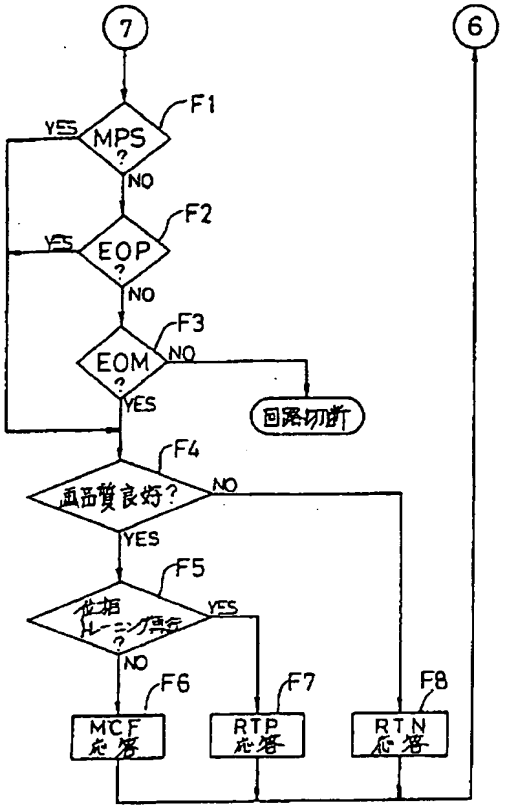
第 11d 図


D1
応答受信?
D2
T1経過?
D3
DCN送出
回路切断
D4
DTC?
D5
DIS?
D6
DCS?
D7
D8
良好?
D9
CFRで応答
D10
FTTで応答
D11
EOM?
D12
T2経過?
D13
メッセージ送出?
D14
命令受信?
D15
トレーニング受信
D16
FAXメッセージ受信
D17
EOM/RTC
D18
メッセージ送出?
1
2
3
4
5
6
7
A

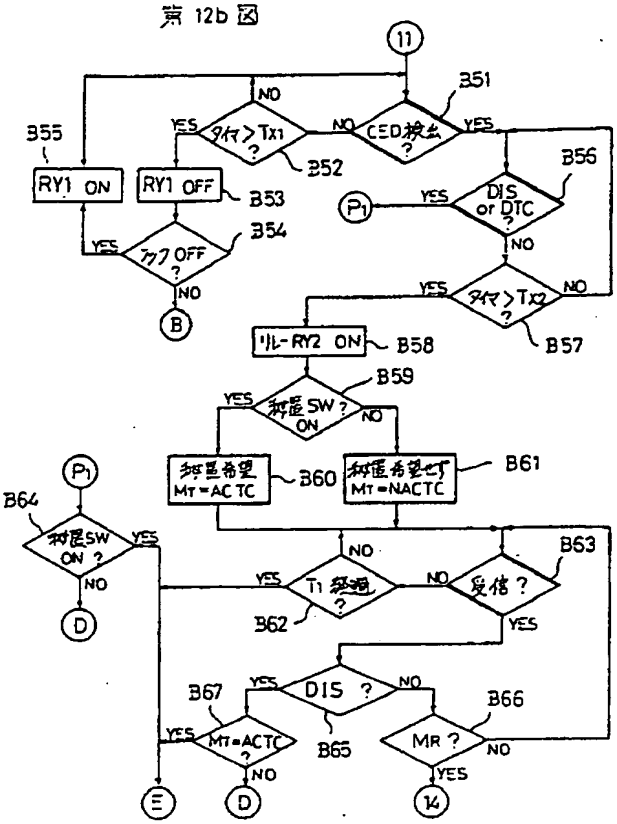
第 11e 図


E1
応答受信?
E2
3回試行?
E3
DCN送出
回路切断
E4
DIS DTC
E5
3回試行?
E6
FTT?
E7
E8
CFR?
E9
トレーニング送出
E10
FAXメッセージ送出
E11
EOM/RTC送出
A
1
2
3
4
5
6
7
8
9

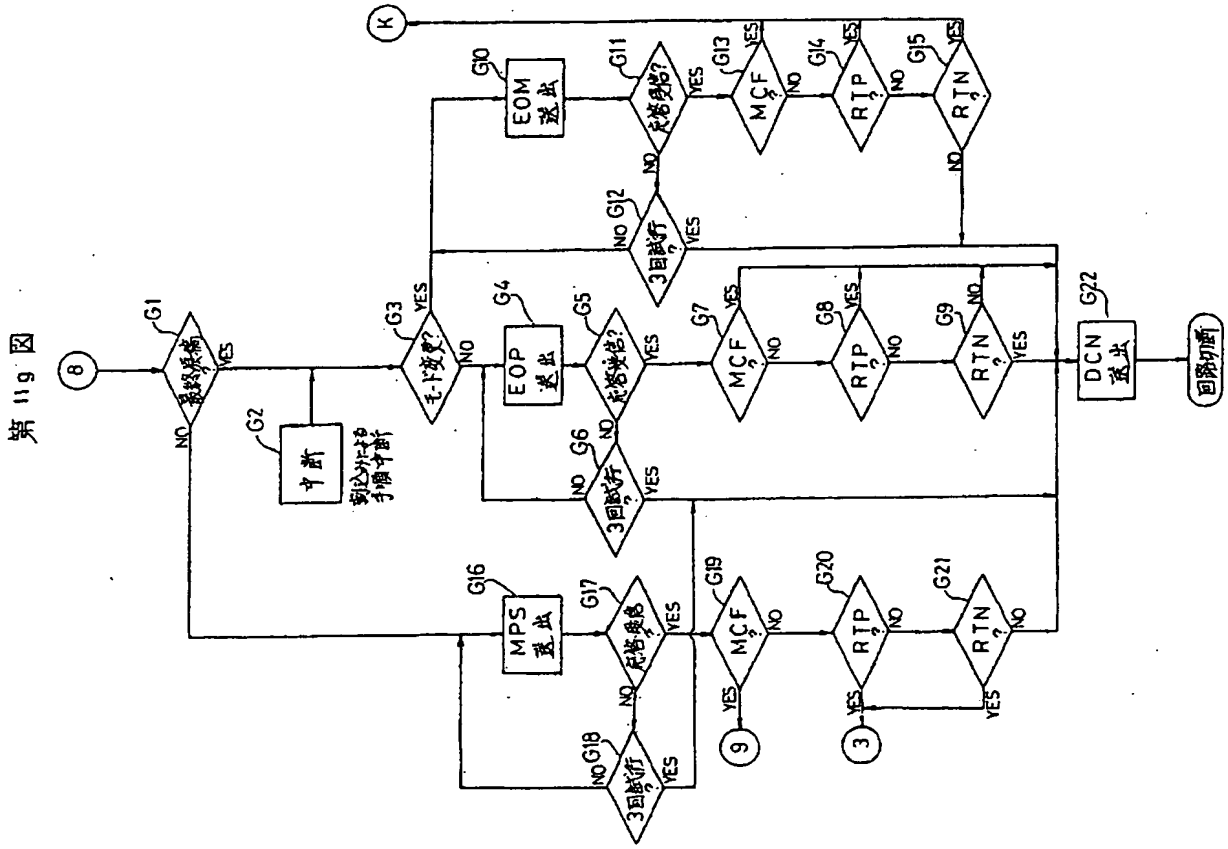
第 11f 図



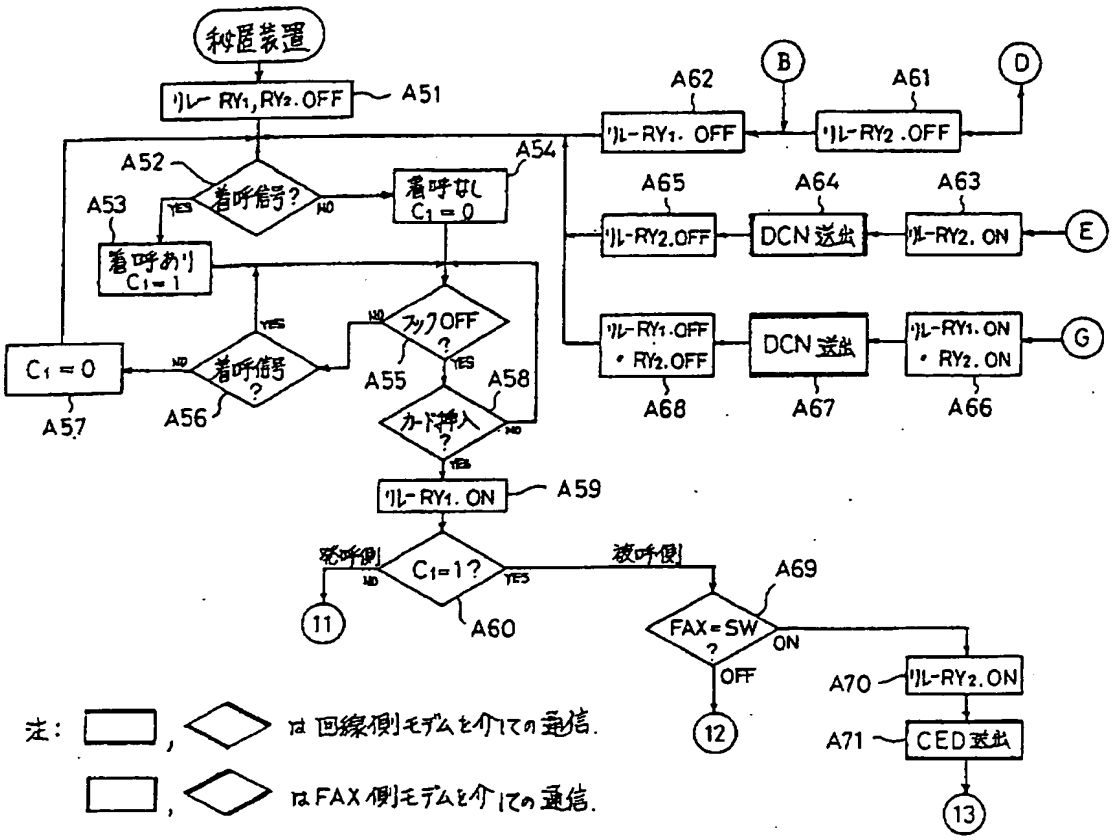
第 12b 図



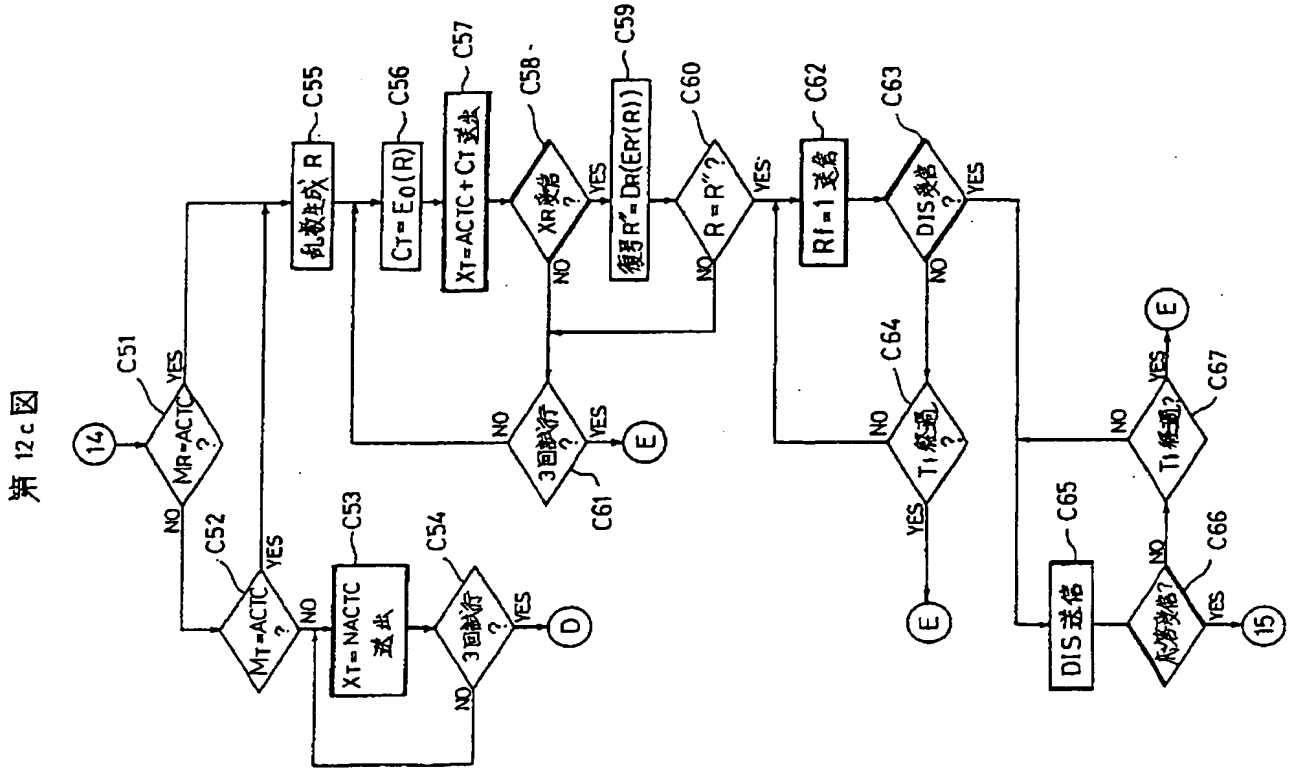
第 11g 図



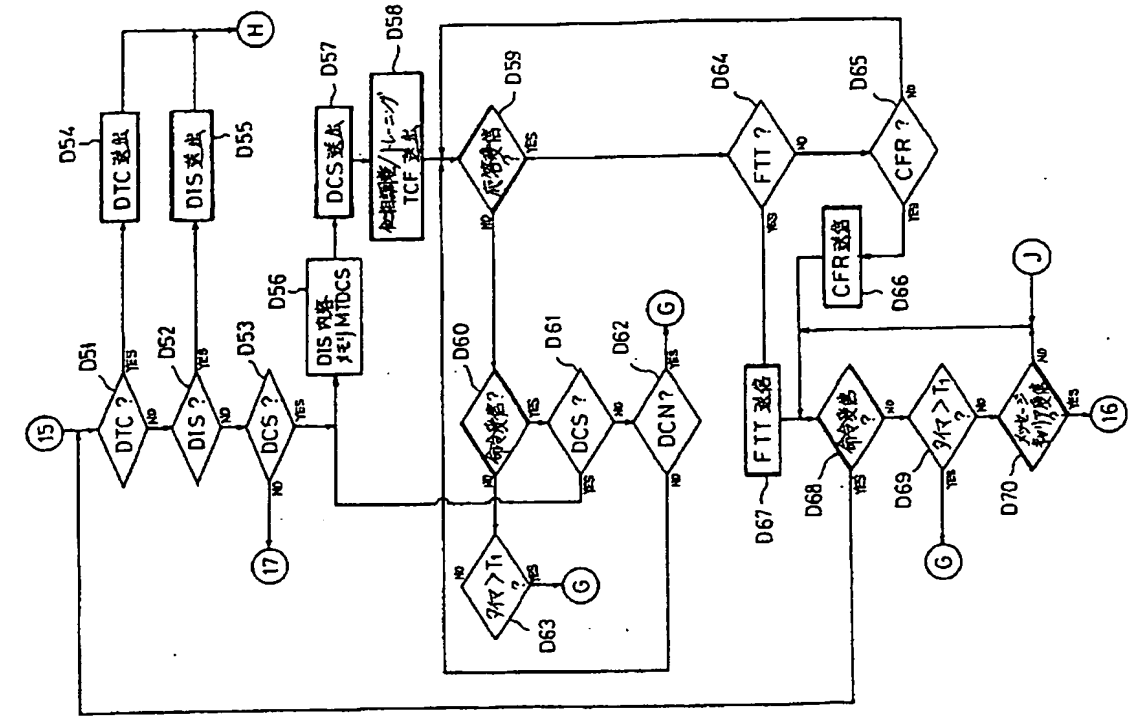
第 12a 図


秘匿装置
リレー RY1, RY2. OFF
A51
A52
着呼信号?
YES
NO
A53
着呼あり C1=1
着呼なし C1=0
A54
フックOFF?
A55
着呼信号?
A56
C1=0
A57
カード挿入?
A58
リレー RY1. ON
A59
C1=1?
A60
受呼側
被呼側
11
A62
リレー RY1. OFF
A61
リレー RY2. OFF
B
D
A65
リレー RY2. OFF
A64
DCN送出
A63
リレー RY2. ON
E
リレー RY1. OFF • RY2. OFF
A68
DCN送出
A67
リレー RY1. ON • RY2. ON
A66
G
FAX=SW?
A69
ON
OFF
12
A70
リレー RY2. ON
A71
CED送出
13
注: , は回線側モデムを介しての通信.
, はFAX側モデムを介しての通信.

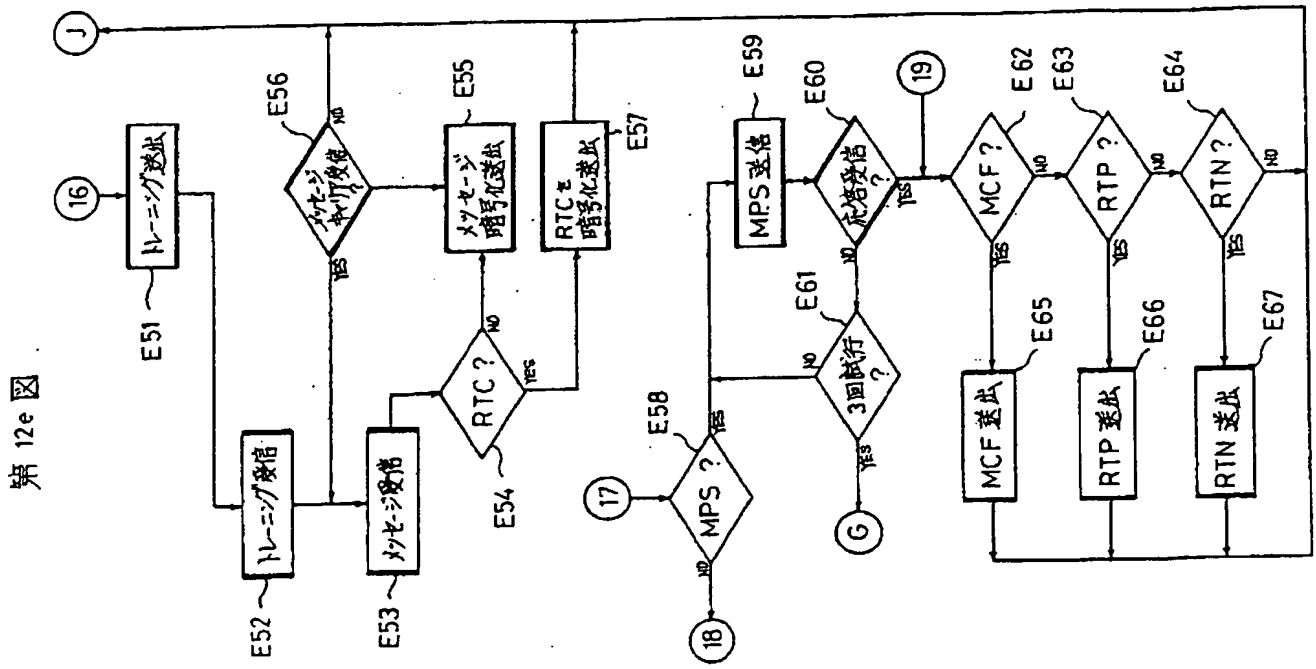
第 12c 図


14
C51
MR=ACTC?
YES
NO
C52
MT=ACTC?
C53
XT=NACTC 送出
C54
3回試行?
C55
乱数生成 R
C56
CT=E0(R)
C57
XT=ACTC+CT 送出
C58
XR受信?
C59
復号R'=DR(ER'(R))
C60
R=R'?
C61
3回試行?
C62
RI=1 送信
C63
DIS受信?
C64
T1経過?
C65
DIS送信
C66
応答受信?
C67
T1経過?
D
E
15

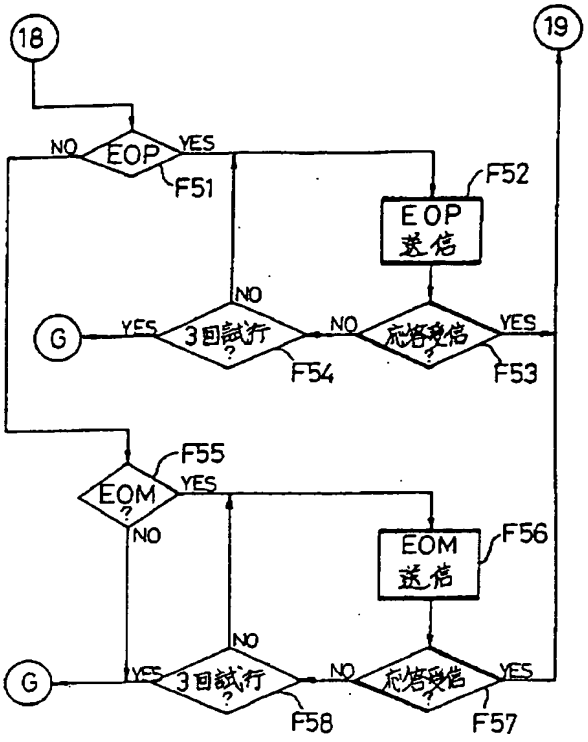
第 12d 図


D51
DTC ?
D52
DIS ?
D53
DCS ?
D54
DTC 送出
D55
DIS 送出
D56
DIS 内容メモリMTDCS
D57
DCS 送出
D58
相互認識/トレーニングTCF 送出
D59
応答有?
D60
命令有?
D61
DCS ?
D62
DCN?
D63
タイマ>T1 ?
D64
FTT ?
D65
CFR ?
D66
CFR 送出
D67
FTT 送出
D68
命令有?
D69
タイマ>T1 ?
D70
メッセージ終了?
15
16
17
G
H
J

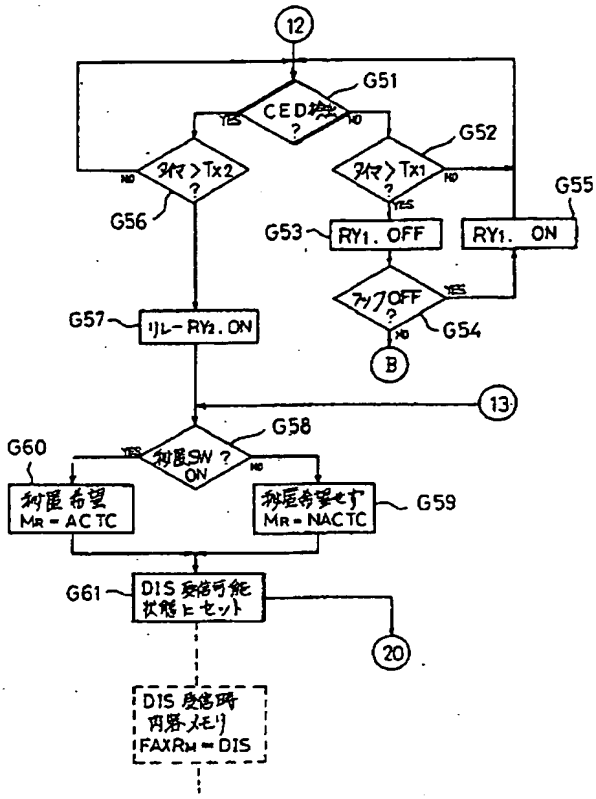
第 12e 図


E51
トレーニング送出
E52
トレーニング受信
E53
メッセージ受信
E54
RTC ?
E55
メッセージ暗号化送出
E56
メッセージ終了?
E57
RTCを暗号化送出
E58
MPS ?
E59
MPS 送信
E60
応答受信?
E61
3回試行?
E62
MCF ?
E63
RTP ?
E64
RTN ?
E65
MCF 送出
E66
RTP 送出
E67
RTN 送出
16
17
18
19
G
J

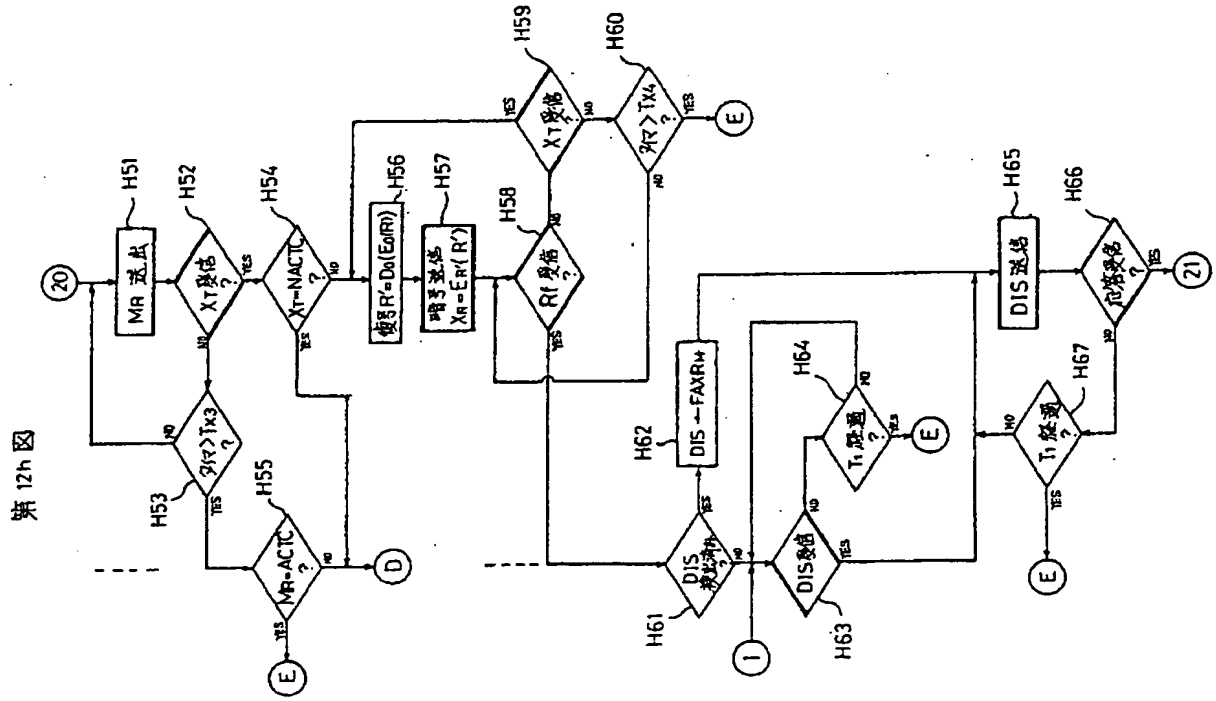
第 12 f 図



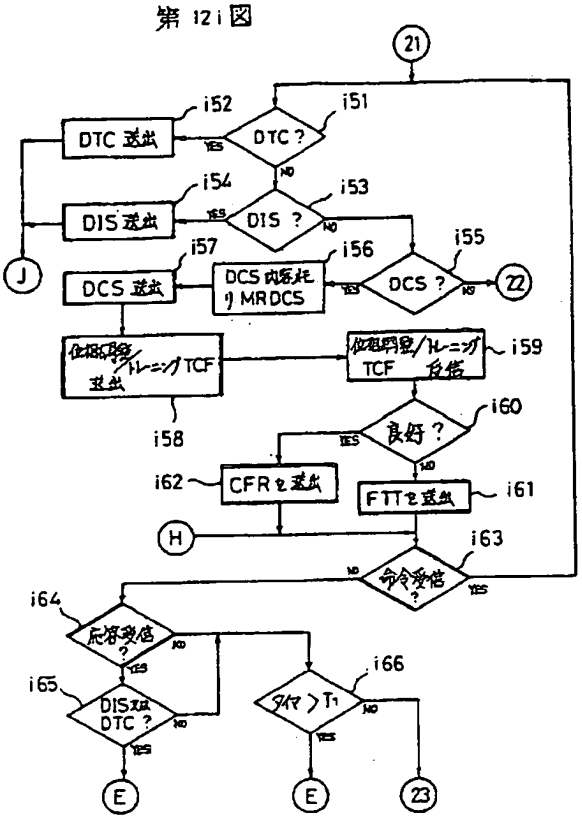
第 12 g 図



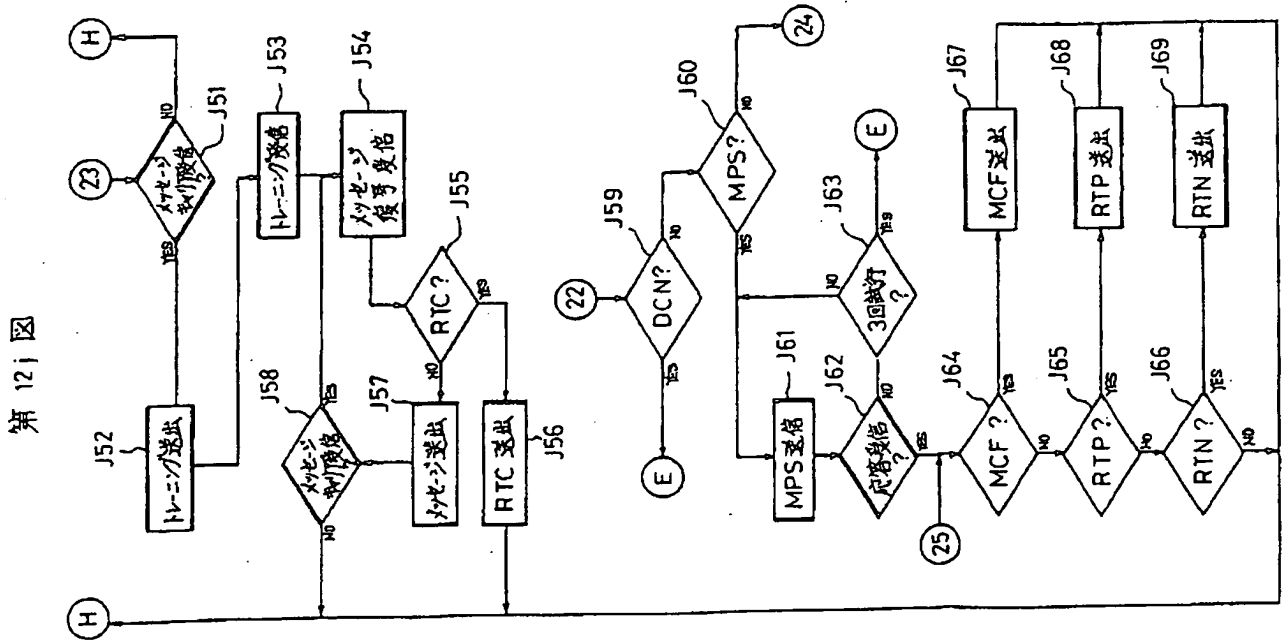
第 12h 図



第 12 i 図


21
i52
DTC 送出
i51
DTC ?
YES
NO
i54
DIS 送出
i53
DIS ?
i55
DCS ?
i57
DCS 送出
i56
DCS 内容比較 / MRDCS
J
22
位相調整 / トレーニング TCF 送出
i58
位相調整 / トレーニング TCF 受信
i59
良好 ?
i60
i62
CFR を送出
FTT を送出
i61
H
i63
命令受信 ?
i64
応答受信 ?
i65
DIS 或は DTC ?
タイマ > T1
i66
E
E
23

第 12 j 図


H
23
J51
メッセージ有り/無し ?
YES
NO
J52
トレーニング送出
J53
トレーニング受信
J54
メッセージ受信
J55
RTC ?
J56
RTC 送出
J57
メッセージ送出
J58
メッセージ有り/無し ?
H
22
J59
DCN?
E
24
J60
MPS?
J61
MPS送信
J62
応答受信 ?
J63
3回試行 ?
E
25
J64
MCF ?
J65
RTP ?
J66
RTN ?
J67
MCF送出
J68
RTP送出
J69
RTN送出